Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act After *United States v. Aleynikov*

By Adam Cohen†

Introduction

Intellectual property regimes must strike an uneasy balance. By offering information owners some degree of exclusive property rights, they provide inventors with an incentive to create and innovate. By placing limits on those rights, they help to ensure that the public has access to the existing body of human knowledge and that a new group of innovators will be able to build on what came before.

Mixed in with this utilitarian formulation is the more normative issue of what rights creators deserve. When intellectual property laws are insufficiently protective of owners' rights, they are criticized for allowing people to unfairly

† Lecturer in Law, Yale Law School and Thomson Reuters Fellow, Yale Information Society Project. J.D. Harvard Law School, *magna cum laude*; A.B. Harvard College, *magna cum laude*.

appropriate innovators' creativity and hard work. When they are too protective, they are faulted for infringing on the public's right to freely consume information and build on what has come before.

It is difficult to find a consensus on when the law has gotten the balance right, but sometimes there is broad agreement on when it has gotten it wrong. Such was the case with the decision of the U.S. Court of Appeals for the Second Circuit in early 2012 reversing Sergey Aleynikov's conviction of theft of trade secrets charges.[1] The consensus was not so much that the Second Circuit's ruling in *United States v. Aleynikov* was wrong–although there were certainly commentators who believed that[2]–but rather that there was something amiss with a trade secrets legal regime that could offer up no law that Aleynikov had violated.

Aleynikov, a Goldman Sachs computer programmer, had been convicted of violating the Economic Espionage Act of 1996 (EEA)[3] and the National Stolen Property Act (NSPA)[4] by stealing his employer's trade secrets.[5] He had accepted a higher-paying job with a rival firm and, on the way out, had stolen a significant portion of the top-secret source code that operated Goldman's high-frequency trading (HFT) system.[6] He later presented it to his new employer.[7]

Aleynikov's actions looked like classic trade secret theft, but the Second Circuit reversed his conviction and ordered him freed.[8] The Second Circuit ruled that the EEA, the main federal trade secret law, prohibited only theft of trade secrets that had been used in products "produced for or placed in" interstate commerce.[9] The court found that Goldman's HFT program, which it used internally and did not sell, did not meet the statute's interstate commerce requirement.[10] The ruling held that the second statute Aleynikov had been convicted under, the NSPA, did not apply because it covered only the theft of tangible "goods," while he had stolen digitized information.[11]

The ruling troubled Wall Street and the technology industry. A *Computerworld* commentary warned that the "disastrous" decision "only

1. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012), *rev'g* 785 F. Supp. 2d 46 (S.D.N.Y. 2011). Aleynikov was later arrested on state charges of unlawful use of secret scientific material. *See* Peter Lattman, *Former Goldman Programmer Is Arrested Again*, N.Y. TIMES, Aug. 9, 2012, http://dealbook.nytimes.com/2012/08/09/ex-goldman-programmer-is-arrested-again.

2. *See infra* note 12 and accompanying text.

3. 18 U.S.C. § 1832 (2006).

4. 18 U.S.C. § 2314 (2006).

5. *Aleynikov*, 676 F.3d at 73.

6. *Id.* at 74, 82; United States v. Aleynikov, 785 F. Supp. 2d 46, 51-54 (S.D.N.Y. 2011).

7. *Aleynikov*, 676 F.3d at 74; *Aleynikov*, 785 F. Supp. 2d at 54.

8. *Aleynikov*, 676 F.3d 71; United States v. Aleynikov, No. 11-1126, 2012 WL 591980, at *1 (2d Cir. Feb. 17, 2012), *rev'g* 785 F. Supp. 2d 46 (S.D.N.Y. 2011) (amended order reversing the judgment of conviction and remanding the matter to the district court to release Aleynikov on bail pending the Second Circuit's opinion).

9. *Aleynikov*, 676 F.3d at 73.

10. *Id.* at 82.

11. *Id.* at 76-79.

encourages other thefts of valuable IT software."[12] The Second Circuit was itself not entirely content with the state of trade secret law that its decision reflected. In a concurring opinion, Judge Calabresi urged Congress to review federal trade secret law and more clearly define what actions it intended to make criminal.[13] There were widespread calls to amend the EEA to cover intellectual property that had not been produced for or placed in interstate commerce. A managing director of one university center on corporate governance and integrity argued that it was "clear that Congress must act to address the electronic transmission of stolen property if the intellectual property theft statutes are to be meaningful in our digital environment."[14]

These calls for expanding the scope of the EEA are half right. The language limiting the EEA to goods that have been produced for or placed in interstate commerce unduly restricts the statute's reach. And the gap it leaves in federal trade secret law is of particular concern in the digital age. A large and growing share of trade secrets, ranging from pure research and development (R&D) to computer codes that run major websites, falls into this category. If the Act is not amended to protect this sort of intellectual property, a key part of the nation's intellectual infrastructure will be unduly vulnerable to theft, putting both individual trade secret holders and the national economy at risk.

The reason these calls are only half right is that from its inception the EEA has had weaknesses that have nothing to do with interstate commerce. Congress enacted the EEA in 1996 with the primary goal of protecting American business against foreign corporate espionage. The section on domestic theft of trade secrets was hastily added, and in drafting it Congress gave insufficient consideration to striking the right balance between underprotecting and overprotecting intellectual property rights.[15] In important respects, Congress wrote a law too tilted in favor of locking down trade secrets and too tilted against the free flow of information.

Congress has begun the process of amending the EEA in response to the *Aleynikov* ruling. The Senate has passed a short bill that simply plugs the

---

12. Bart Perkins, *U.S. Appeals Court Has Compromised Software Rights*, COMPUTERWORLD (May 7, 2012, 6:00 AM), http://www.computerworld.com/s/article/9226856/Court_Has_Compromised_Software_Rights; *see also* Brad Reid, *Electronically Transmitted Source Code Not Stolen Goods Under the National Stolen Property Act*, HUFFINGTON POST (Apr. 13, 2012, 2:03 PM), http://www.huffingtonpost.com/brad-reid/electronically-transmitte_b_1423645.html (arguing that the *Aleynikov* ruling "indicates the need to revise U.S. federal intellectual property theft statutes"); Peter J. Toren, *An Analysis of Economic Espionage Act Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!*, BLOOMBERG BNA'S PAT., TRADEMARK, & COPYRIGHT J. 8, 10 (Sept. 21, 2012), http://petertoren.com/wp-content/uploads/2012/10/toren-eea2.pdf ("Congress should amend the EEA so as to remove any doubt that trade secrets that are related to products or processes and that are used internally are protected to the extent permitted by the Commerce Clause. There is simply no reason to limit the EEA any further beyond that required by the Commerce Clause.").

13. *Aleynikov*, 676 F.3d at 83 (Calabresi, J., concurring).

14. Reid, *supra* note 12.

15. *See infra* notes 110-113 and accompanying text.

interstate-commerce hole.[16] What Congress has not done, however, is to undertake a careful, deliberative inquiry into how the EEA fits into the broader framework of intellectual property laws–something it also failed to do in 1996. Rather than rushing to correct one high-profile problem, Congress should give greater consideration to all of the EEA's deficiencies. In the end, Congress should produce a statute that is more protective of trade secrets in some respects, less protective in others, and more carefully calibrated to the important societal interests at stake.

I. Protecting Trade Secrets

A. Theft of Trade Secrets

Confidential, valuable commercial information–trade secrets–is a large part of the U.S. economy. It is difficult to quantify precisely how large, in part because the information is by definition secret. But by some estimates, as much as seventy percent of American firms' market value may lie in intellectual property, a significant part of which is trade secrets.[17]

Trade secrets are more vulnerable to theft than physical assets such as heavy equipment. They are frequently easy to access; they can generally be transported without much difficulty, often through a simple Internet communication; and they are sometimes carried away in the thief's own memory.[18]

There are no concrete figures for the value of trade secrets stolen annually. Trade secret thefts often go undetected and when companies are aware that trade secrets have been taken there can be business reasons for not going public. Some estimates have placed the economic damage of trade secret thefts at as much as $300 billion per year.[19] When FBI Director Louis Freeh testified to Congress in support of the EEA, he stated that over one million jobs might have been lost from stolen intellectual property, a substantial portion of which was trade secrets.[20]

---

16. Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (as passed by Senate, Nov. 27, 2012).

17. *See* Carl Pacini & Raymond Placid, *The Importance of State Trade Secret Laws in Deterring Trade Secret Espionage*, 7 BUFF. INTELL. PROP. L.J. 101, 102 (2009).

18. JAMES POOLEY, TRADE SECRETS § 13.01 (1997).

19. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., NCIX 2003-10006, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE–2002 at 2 (2003), http://www.fas.org/irp/ops/ci/docs/2002.pdf; *see also* POOLEY, *supra* note 18, § 13.01 ("[B]ecause the property usually remains available to the victim, the theft may be extremely difficult to detect absent forensic computer inspections.").

20. *Economic Espionage: Hearing Before the S. Select Committee on Intelligence & the Subcomm. on Terrorism, Tech., and Gov't Info. of the S. Comm. on the Judiciary*, 104th Cong. 10 (1996) (prepared statement of Louis Freeh, Dir., Fed. Bureau of Investigation).

Cases that have gone to trial give an indication of how high the stakes can be. In *United States v. Hsu*,[21] an FBI sting operation caught a pair of Taiwanese business people attempting to steal the processes, methods, and formulas used to manufacture the Bristol-Meyers anti-cancer drug Taxol. At the time, Taxol had an estimated $400 to $600 million in annual worldwide retail sales.[22] In the *Aleynikov* case, the stolen HFT source code supported three Goldman business lines that generated a net pretax income of approximately $300 million a year.[23]

Trade secret theft can devastate a business. In a recent high-profile case, American Superconductor, a Massachusetts wind-energy company, had important trade secrets stolen by its largest customer, Sinovel, a Chinese wind turbine manufacture. Sinovel's purchases had constituted more than seventy percent of American Superconductor's revenues. But in 2011, Sinovel suddenly began refusing shipments of American Superconductor's wind turbine electric systems and software. It was later revealed that the Chinese company had offered an American Superconductor employee $1.5 million to steal key software. After Sinovel pulled its business, American Superconductor's stock price fell more than eighty percent.[24]

The American Superconductor case demonstrated not only how great the impact of trade secret theft can be, but also how vulnerable industry has become to theft in the modern economy. Companies are increasingly global, with far-flung workforces that in many cases have looser ties and less loyalty to central management. Competitors are also increasingly global, and a foreign-based company may believe itself less likely to be caught and punished than an American company would be. And with so much of a company's value tied up in information that can be stolen on a computer disk or transferred in an e-mail, major thefts can be carried out quickly and unobtrusively.

Many companies have seen, as American Superconductor did, that a single well-placed employee who acts disloyally can do tremendous damage.[25] The defendant in *United States v. Chung*,[26] an engineer who worked for Boeing, had accumulated more than 300,000 pages of confidential documents, most of which he was stowing in an unfurnished storage area under his home. The documents contained sensitive information related to the space shuttle, the F-15 Fighter, the B-52 Bomber, and the Chinook Helicopter.[27] Chung's cache

---

21. 155 F.3d 189 (3d Cir. 1998).

22. MATTHEW SUFFNESS, TAXOL: SCIENCE AND APPLICATIONS 89 (1995).

23. Brief for Defendant-Appellant at 6, United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012) (No. 11-1126-cr).

24. Jonathan Weisman, *U.S. to Share Cautionary Tale of Trade Secret Theft With Chinese Official*, N.Y. TIMES, Feb. 14, 2012, http://www.nytimes.com/2012/02/15/world/asia/chinese-official-to-hear-trade-theft-tale.html.

25. *Id.*

26. 659 F.3d 815 (9th Cir. 2011).

27. *Id.* at 819.

also included trade secrets concerning the Delta IV Rocket and a phased array antenna for the space shuttle.[28]

B. The Rise of Trade Secret Law

The principle that the theft of trade secrets should be actionable at law has deep historical roots. Ancient Rome's *actio servi corrupti* created a legal cause of action for the "corruption" of slaves by bribery or intimidation, and such corruption may have included enticing slaves to communicate their owners' business secrets.[29] In the Renaissance, legal protections for certain kinds of trade secrets emerged across Europe.[30] In Anglo-American law, however, recognition of a cause of action for damages for theft of trade secrets was slow in coming. Patents and copyrights were well established in Europe when the American Republic was founded. They were expressly provided for in the Constitution and protected by early statutes.[31] Trade secrets, by contrast, were not protected in America until the nineteenth century.[32]

There were attempts by courts to recognize a cause of action for trade secret theft as early as the 1830s,[33] but it was not until after the Civil War that an American court first tried to articulate a full rationale for the offense. In the seminal case of *Peabody v. Norfolk*[34] in 1868, the Massachusetts Supreme Court ruled that Peabody's former employee, Norfolk, had wronged him by stealing a secret industrial process for making gunny cloth and delivering it to a competitor. The ruling was vague about the precise basis for the legal claim, which befitted an area of law that would be theoretically challenged for many years to come. The *Peabody* Court asserted that businesses have a property interest in trade secrets:

> It is the policy of the law for the advantage of the public, to encourage and to protect invention and commercial enterprise. If a man establishes a business and makes it valuable by his skill and attention, the good will of that business is recognized by the law as property.[35]

---

28. *See id.* at 823.

29. A. Arthur Schiller, *Trade Secrets and the Roman Law; The* Actio Servi Corrupti, 30 COLUM. L. REV. 837, 838-43 (1930). This history has been contested. *See* Alan Watson, *Trade Secrets and Roman Law: The Myth Exploded*, 11 TUL. EUR. & CIV. L.F. 19 (1996).

30. *See* S.R. Epstein, *Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe*, 58 J. ECON. HIST. 684, 691-94 (1998); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 315 n.8 (2008).

31. *See* U.S. CONST. art. 1, § 8, cl. 8 ("To promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries . . . ."); Copyright Act of 1790, 1 Stat. 124 (codified as amended at 17 U.S.C. §§ 101-1332 (2006)) (establishing copyright system); Patent Act of 1790, 1 Stat. 109 (codified as amended at 35 U.S.C. §§ 1-376 (2006)) (authorizing the issuance of patents).

32. *See* Lemley, *supra* note 30, at 315.

33. Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 70 (1999).

34. 98 Mass. 452 (1868).

35. *Id.* at 457.

At the same time, the court emphasized that a relationship of trust had been violated. A court of chancery will protect property, Justice Gray said, "against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons."[36] The *Peabody* Court could be seen as basing liability on property, breach of contract, tort, or some combination of all three.

After *Peabody*, the common law right of action for theft of trade secrets became increasingly established, but no general agreement emerged on what the basis was for the offense. In the 1917 case of *E.I. du Pont de Nemours Powder Co. v. Masland*,[37] the Supreme Court came down in favor of the breach-of-relationship argument. The Court upheld an injunction barring the defendant from disclosing secret processes that he had acquired while working for du Pont. Writing for the Court, Justice Holmes stated that the "starting point for the present matter" was "not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs."[38]

This understanding of the nature of trade secrets theft was reflected in the Restatement (First) of Torts, which was issued in 1939. The Restatement stated that the idea of trade secrets as property had been "frequently advanced and rejected."[39] The tort–and it was significant that it was being characterized as a tort–turned instead on a "general duty of good faith." What mattered in evaluating an appropriation of secret business information was whether it had been taken through "improper means" or learned of when confidential matters were disclosed by mistake.[40] The "improper means" that the Restatement looked for included "means which fall below the generally accepted standards of commercial morality and reasonable conduct."[41] In the vision of the Restatement, the question was not whether property was stolen but rather whether the defendant violated "commercial morality" and "reasonable conduct."

In time, this malfeasance-based view of trade secret theft went into retreat, and the law looped back toward a property-based theory. In the 1984 case of *Ruckelshaus v. Monsanto*,[42] the Supreme Court considered whether Monsanto had a property interest protected by the Fifth Amendment's Takings Clause in the health, safety, and environmental data that it had submitted to the Environmental Protection Agency. Noting that trade secrets possess "many of the characteristics of more tangible forms of property," including being assignable and passing to a trustee in bankruptcy, the Court ruled that they must

---

36. *Id.* at 458.
37. 244 U.S. 100 (1917).
38. *Id.* at 102.
39. Michael Simpson, Note, *Future of Innovation: Trade Secrets, Property Rights, and Protectionism–An Age Old Tale*, 70 BROOK. L. REV. 1121, 1142 (2005).
40. *See* RESTATEMENT (FIRST) OF TORTS § 757 (1939).
41. *Id.* § 757 cmt. f at 11.
42. 467 U.S. 986 (1984).

be considered property for purposes of the Takings Clause.[43] Lower courts also took a property-focused approach, ruling that people who take trade secrets should be punished like any other kind of thief.[44]

While courts struggled to settle on a definitive rationale for the offense of trade secret theft, commentators took note of the theoretical incoherence. They described trade secret law as a "puzzle"[45] and a "doctrine in search of justification,"[46] and debated whether it should properly be viewed as a subset of property,[47] contract,[48] privacy law,[49] or–as the Restatement suggests–tort.[50] One influential commentator has argued that it is pointless to seek out distinct intellectual underpinnings for trade secret law, since it is properly viewed not as an autonomous legal regime, but rather as "a collection of other legal wrongs."[51]

As the courts now frame it, trade secrets have come to look not like ordinary property, but rather like a subset of intellectual property.[52] Judges often analyze the protection of trade secrets the way they analyze protecting patent or copyright, emphasizing the social benefits of rules that promote innovation. In *Kewanee Oil Co. v. Bicron Corp.*,[53] the Supreme Court ruled that Ohio's state trade secret law was not preempted by federal patent law. In describing the purpose of trade secret laws, the court cited maintaining commercial ethics, but also trade secret laws' role in providing "another form of incentive to invention."[54] In a later case, *Aronson v. Quick Point Pencil Co.*,[55] the Court noted that trade secret law helps to ensure that "the public is not deprived of the use of valuable, if not quite patentable," inventions.[56]

---

43. *Id.* at 1002-04.

44. *See* University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 542-44 (discussing wrongful appropriation of computer program as "theft"); 3 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS § 12.06 (2008).

45. Lemley, *supra* note 30, at 312.

46. Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (March 1998).

47. Miguel Deutch, *The Property Concept of Trade Secrets in Anglo-American Law: An Ongoing Debate*, 31 U. RICH. L. REV. 313 (1997).

48. *See, e.g.*, David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 70-71 (1991) (using contract rationale in discussing trade secret law).

49. Bruce T. Atkins, Note, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L., REV. 1151 (presenting trade secret law as a privacy right).

50. *See* RESTATEMENT (FIRST) OF TORTS § 757 (1939).

51. Bone, *supra* note 46, at 245-46.

52. *See, e.g.*, Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 9 (1998); Lemley, *supra* note 30, at 313.

53. 416 U.S. 470 (1974).

54. *Id.* at 484.

55. 440 U.S. 257 (1979).

56. *Id.* at 266 (citing *Kewanee*, 416 U.S. at 485).

There are, in fact, strong similarities between trade secret law and patent and copyright law. All three are designed to protect information that society believes certain people have a proprietary right to. All three regimes set out specific conditions owners must take to win legal protection. In the case of trade secrets, the three basic requirements are that the owners must (1) have information that meets specifications set out in the law; (2) the information must be valuable to its owner; and (3) the owner must have taken appropriate steps to keep it secret.[57]

All three regimes are also concerned, as the *Kewanee* Court recognized, with promoting innovation. Operating R&D departments, employing scientists and computer programmers, and creating new business processes can be expensive. If business innovations are not protected against competitors, the utilitarian theory of trade secrecy posits that businesses will have less incentive to invest in such innovations.[58]

Innovation is important not only for companies, but for society as a whole. Economists have explained the critical role that innovation plays in economic growth and national prosperity. Joseph Schumpeter extolled the entrepreneur as an innovative force and "the pivot on which everything turns."[59] There is a sizable body of economic analysis indicating that R&D spending has a strong positive effect on productivity.[60]

For all of the similarities between trade secret law and patent and copyright, there are also significant differences. The most basic one is secrecy. To protect a patent or copyright, an innovator is required to register the discovery and make it public.[61] The trade secret owner is required to do the opposite: make appropriate efforts to prevent his innovation from becoming known.[62]

Another factor setting trade secrets apart from patents and copyright is that the subject matter that can be protected is broader. Patents can only be obtained for discoveries that are "novel" and "non-obvious."[63] Copyright is only available for expression, not underlying ideas or facts.[64] Trade secrets are

---

57. Simpson, *supra* note 39, at 1123.

58. David S. Levine, *The People's Trade Secrets*, 18 MICH. TELECOMM. TECH. L. REV. 61, 71 (2011).

59. *See* JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY (3d ed. 1950); *see also* THOMAS K. MCCRAW, PROPHET OF INNOVATION: JOSEPH SCHUMPETER AND CREATIVE DESTRUCTION (2007).

60. *See, e.g.*, Frank Lichtenberg & Donald Siegel, *The Impact of R&D Investment on Productivity—New Evidence Using Linked R&D-LRD Data*, 29 ECON. INQUIRY 203 (1991).

61. *See* 17 U.S.C. § 412 (2006) (registration of copyright a prerequisite to certain remedies for infringement); 35 U.S.C. § 111 (2006) (setting forth procedures for applying for patent).

62. Professor Landes and Judge Posner have argued that the expenditures on securing a trade secret should be in proportion to the value of the information being protected. WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 357 (2003); Pacini & Placid, *supra* note 17, at 108.

63. 35 U.S.C. §§ 102, 103 (2006).

64. 17 U.S.C. § 102 (2006).

not limited in these respects. A trade secret can consist of information as mundane as customer lists or delivery routes.[65] There are also important differences in lifespan. Patents and copyrights are of limited duration, after which the right to the information reverts to the public.[66] Trade secrets have no such limits: they can conceivably last forever.

These differences between trade secrets and other forms of intellectual property suggest some of the concerns inherent in formulating trade secret law–in particular, the challenges in striking a proper balance between what is protected and what is not. Innovators who take advantage of trade secret protection have not participated in what Professor Dreyfuss has called the traditional "intellectual property bargain:" disclosing information in exchange for a monopoly over its use.[67] In this respect, trade secret laws do not contribute to the march of human knowledge by making information public and preparing for the day when it will enter the public domain. Instead, they wall information off.

Although trade secret laws keep information from the public, potentially for great lengths of time, they can nevertheless promote innovation. The 7th Circuit, in an opinion authored by Judge Posner, has observed that patent protection is expensive and temporary, and these hurdles can make such safeguards unattractive to some innovators. If innovators were protected only when they took "extravagant, productivity-impairing measures to maintain their secrecy," he argues, "the incentive to invest resources in discovering more efficient methods of production would be reduced, and with it the amount of invention."[68] For a discrete set of innovations, trade secret laws can promote "productive measures" that might not occur under a pure patent and copyright regime.[69]

Still, walling off innovations is a legitimate concern about trade secret law. So is the absence of a time limit by which the rights to the innovations must be shared. Patents are relatively short in duration. Copyrights last longer, but ultimately the information they protect is supposed to enter the public domain. A trade secret has the potential to remain the exclusive property of its owner forever. A final concern about trade secret law is the expansive definition of what can qualify for protection. Patents and copyrights have inherent limitations, having to be, respectively, novel and expressive. Not being restricted in that way, the definition of a trade secret can be more far-reaching–

65. Simpson, *supra* note 39, at 1123.

66. 35 U.S.C. § 154 (2006) (setting duration of patents at twenty years in most cases); 17 U.S.C. §§ 302-05 (2006) (setting forth duration of copyrights depending on circumstances of the copyright).

67. Dreyfuss, *supra* note 52, at 1.

68. Rockwell Graphic Sys. Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

69. Iraj Daizadeh et al., *A General Approach for Determining When to Patent, Publish, or Protect Information as a Trade Secret*, 20 NATURE BIOTECHNOLOGY 1053, 1053 (2002).

extending to almost any kind of business matter–and runs the risk of taking in more information than is socially desirable.

C. The Statutory Regime Before 1996

The trade secret law that emerged was–despite the best efforts of the drafters of the Restatement–an awkward patchwork. The definitions of what counted as a trade secret were vague, and varied considerably from state to state. Citing the "doubtful and confused status" of the law,[70] in 1979 the National Conference of Commissioners on Uniform State Laws adopted a model state law, the Uniform Trade Secrets Act (UTSA).

The UTSA not only sought to make state trade secret laws more uniform, it also imposed a distinct vision on them. While the 1939 Restatement applied only to material "continuously used" in a business, the UTSA dropped that requirement.[71] Under the model state law, even if a business had not yet done anything with an idea, it could still protect it.[72] The UTSA also contained a more expansive list of kinds of information that could be trade secrets, including such categories as "program[s]," "process[es]," and "technique[s]."[73] States largely embraced the UTSA model law, and 47 states enacted statutes based on it.[74]

The UTSA did not shore up all of the perceived problems with state trade secret laws. There remained a lack of uniformity, not only because of the three holdout states, but also because even in the adopting states the wording and interpretations of state trade secret statutes varied significantly. Many state statutes still required a plaintiff to show that a trade secret had been acquired by "improper means," which limited their use in many cases.[75]

Beyond difficulties with the statutes, there were other problems with relying on state civil actions to address theft of trade secrets. Corporations were often reluctant to take on the effort and expense of suing, particularly in the

---

70. UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS 1 (Nat'l Conference of Comm'rs on Unif. State Laws 1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (citing Comment, *Theft of Trade Secrets: The Need for a Statutory Solution*, 120 U. PA. L. REV. 378, 380-81 (1971)).

71. *See* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 869-70 (2002); Pacini & Placid, *supra* note 17, at 105.

72. Symposium, *Panel III: Trade Secrets and Other Avenues for Protection of Advanced Technology*, 20 FORD. INTELL. PROP. MEDIA & ENT. L.J. 875, 880 (2010) (comments of Roger Milgrim).

73. UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 438 (1990); *see* Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 433-34 (1995).

74. *See* Michael Scalera & Joan T. Kluger, *New Jersey Adopts Uniform Trade Secrets Act: Implications for Your Intellectual Property Portfolio*, SCHNADER HARRISON SEGAL & LEWIS LLP 1 (Jan. 2012), http://www.schnader.com/files/Uploads/Documents/IP%20Alert_New%20Jersey%20Adopts%20Uniform%20Trade%20Secrets2012.pdf.

75. *See* Aaron Burnstein, *A Survey of Cybercrime in the United States*, 18 BERKELEY TECH. L.J. 313, 323 (2003).

case of smaller companies for whom the cost of litigation could be prohibitive.[76] Individuals who stole trade secrets were often judgment proof, removing the incentive for victims to sue.[77] And even if a civil action succeeded, the remedy was often not sufficient to compensate for the loss of a valuable trade secret.[78]

Running parallel to this civil system, many states made theft of trade secrets a crime, either through dedicated trade secret statutes or through their general theft laws.[79] State criminal law also proved to have its limits. Definitions of trade secret theft in state criminal laws are generally narrow. They often apply only when there is a taking of a physical thing, such as a document or a computer disk. In many cases, the penalties imposed are relatively light. State prosecutors also commonly lack the resources to take on complex trade secrets theft cases, and cannot call on the Federal Bureau of Investigation and the "extensive networks" that U.S. Attorney's Offices have at their disposal.[80] Not least, for many state prosecutors theft of trade secrets is not a priority.[81] They have used the criminal law "sparingly," preferring to let victims of trade secret theft enforce the law through private civil actions.[82]

Prior to 1996, trade secret theft was sometimes prosecuted at the federal level using laws that were not specific to trade secrets. The most commonly used statute was the NSPA,[83] a Depression-era law aimed at organized crime rings that stole things of value, including stock certificates, and fenced them across state lines. The NSPA makes it illegal to "transport[], transmit[], or transfer[] in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more . . . ."[84]

The NSPA had an inherent weakness: its limitation to "goods, wares, merchandise, securities, or money." This catchall phrase was drafted at a time when the scope of things that could be stolen was more limited. There were no

76. *See* MILGRIM & BENSEN, *supra* note 44, § 12.06[4] ("To abdicate government responsibility in this area . . . would operate as a kind of denial of due process of the law. Whereas large industrial corporations can afford and might be willing to expend the large sums that a trade secret civil action might entail, many smaller companies, with secrets proportionately as valuable to them as secrets of the larger companies, often cannot.").

77. *See* United States v. Hsu, 155 F.3d 189, 194 n.7 (3d Cir. 1998).

78. James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 186 (1997).

79. *See* MILGRIM & BENSEN, *supra* note 44, § 12.06[1]; Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 286 (1999); Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921, 931 (1989).

80. POOLEY, *supra* note 18, § 13.03[6].

81. *See* Pooley et al., *supra* note 78, at 205; *see also* POOLEY, *supra* note 18, § 13.03[6] ("By contrast, the FBI and U.S. Attorney's office have extensive networks and other resources that are difficult to match.").

82. Moohr, *supra* note 71, at 872.

83. 18 U.S.C. § 2314 (2006).

84. *Id.*

computers, no copying machines, no biotechnology, and the concept of intellectual property was far more limited.[85]

For decades, prosecutors had mixed success in pursuing people under the NSPA for stealing intellectual property when no physical good was stolen. There were cases in which federal courts ruled that theft of intangible goods was covered by the NSPA, notably a ruling by the U.S. Court of Appeals for the Ninth Circuit in 1983 that copying sound and video recordings could violate the Act,[86] but the question was far from settled.

In the 1985 case *Dowling v. United States,*[87] the Supreme Court set out a more restrictive interpretation of what kinds of property are covered by the NSPA. In *Dowling*, the Court said that the NSPA does not "plainly and unmistakably" cover the interstate transport of bootleg records.[88] The Act clearly contemplates a physical identity between the items unlawfully taken and the ones that are transported, the Court said, and that requires a physical taking.[89] The *Dowling* ruling left enough room for interpretation that some lower courts have continued to allow prosecutions under the NSPA even in cases where there was no physical good taken,[90] but a physicality requirement is widely imposed.[91] It increasingly became clear that when they tried to use the NSPA when the physicality condition was not met "prosecutors were trying to fit a square (intangible secrets) peg into a round (tangible goods) hole."[92]

There were other federal statutes that could be and were used to prosecute theft of trade secrets, notably federal mail and wire fraud statutes.[93] The mail and wire fraud statutes do apply to thefts of "property," which includes intangible forms of property,[94] but they have other limitations. These laws apply only when the theft was done with the use of postal mail or wire transmissions.

The courts have interpreted this condition broadly. In a criminal prosecution of a *Wall Street Journal* reporter, the Supreme Court ruled that the

---

85. S. REP. NO. 104-359, at 10 (1996).

86. *See, e.g.*, United States v. Belmont, 715 F.2d 459, 462 (9th Cir. 1983) ("In view of the clear intent of Congress to treat the wrongful copying of sound and video tapes and motion picture materials as a species of theft, it is only logical to hold that the interstate transportation of the stolen copies is a violation of § 2314.").

87. 473 U.S. 207 (1985).

88. *Id.* at 228.

89. *Id.* at 214-16.

90. *See, e.g.*, United States v. Riggs, 739 F. Supp. 414, 420 (N.D. Ill. 1990) (applying NSPA to transfer of text file). The district court noted that if the data had been taken on a floppy disk or printed out and carried over state lines it would fall under the statute, and said that the result should be the same when the defendant "stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferable, accessible, even salable form." *Id.* at 421.

91. *See, e.g.*, United States v. Brown, 925 F.2d 1301, 1307-08 (10th Cir. 1991) (stating that the *Riggs* decision was "in error" in light of *Dowling*).

92. POOLEY, *supra* note 18, § 13.03[1].

93. 18 U.S.C. §§ 1341, 1343 (2006).

94. *See, e.g.*, United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (applying wire fraud statute to theft of computer software).

fact that the newspaper was delivered by mail and wire brought the reporter's actions under the mail and wire fraud statutes.[95] But these laws cannot be used in the substantial number of trade secret cases in which mail or wire are not used. The mail and wire fraud statutes also have fraud as a necessary element. They have been held not to apply to trade secret cases in which the misappropriated information was taken by unauthorized copying, with no specific act of fraud attached.[96] The "frustration" that prosecutors and theft victims experienced in dealing with these laws contributed to calls for a dedicated federal criminal trade secrets statute.[97]

D. The Economic Espionage Act

In the early 1990s, a number of factors combined to create momentum for a federal criminal trade secret law. There was widespread agreement among law enforcement and businesses that the federal and state laws that were already on the books did not adequately protect trade secrets. A federal law could provide a nationwide solution.

There was also concern that newly ascendant global forces were contributing to a rise in trade secret theft. The end of the Cold War, some analysts said, meant that military and political spies–who were less in demand for political work–would begin to direct their efforts to industrial espionage, where demand remained strong.[98] In fact, there were reports that industrial espionage was on the rise, particularly by foreign governments and their agents.[99] The FBI said that it was "investigating reports and allegations of economic espionage against the United States by individuals or organizations from 23 different countries."[100] The business community wanted to protect its intellectual property against this threat, and members of Congress wanted to defend the nation's industrial and technological edge.

There was also, in the early 1990s, a strong push to use criminal law to punish theft of intellectual property.[101] Congress was in the midst of enacting a series of federal criminal statutes to address the problem. In 1984, it criminalized trademark infringement with the Trademark Counterfeiting Act.[102] In 1992, Congress expanded criminal liability for copyright infringement with

95. *See* Carpenter v. United States, 484 U.S. 19, 28 (1987).

96. Pooley et al., *supra* note 78, at 180.

97. POOLEY, *supra* note 18, § 13.03[1].

98. Nicola Searle, *The Criminalization of the Theft of Trade Secrets: An Analysis of the Economic Espionage Act*, 2 IP THEORY 33, 34 (2012), http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1011&context=ipt.

99. *See* Simpson, *supra* note 39, at 1126.

100. H.R. REP. NO. 104-788, at 5 (1996), *quoted in* Coblenz, *supra* note 79, at 283 n.247.

101. Benjamin K. Sovacool, *Placing a Glove on the Invisible Hand: How Intellectual Property Rights May Impede Innovation in Energy Research and Development (R&D)*, 18 ALB. L.J. SCI. & TECH. 381, 436 (2008).

102. Pub. L. No. 98-473, 98 Stat. 2178 (codified as amended at 18 U.S.C. § 2320 (2006)).

the Copyright Felony Act.[103] In 1996, it enacted the Anticounterfeiting Consumer Protection Act,[104] which made trademark counterfeiting and copyright violations predicate acts under Racketeer Influenced and Corrupt Organization (RICO) and money laundering statutes. And in 1998, it passed the Digital Millennium Copyright Act,[105] which made it illegal to sell or use devices that circumvent technological protections of copyrighted materials.

Finally, changes in technology were leading Congress and business leaders to worry more than ever about protecting their intellectual property. Workplaces were changing. More employees were working from virtual offices, and there were more collaborative engineering projects. There was more outsourcing. And growing integration of the Internet into business was making it easier to move information around. Valuable trade secrets were more vulnerable than ever before.[106]

On October 11, 1996, President Bill Clinton signed the EEA.[107] Congress's focus in passing the law was foreign industrial espionage, and it originally intended to limit the statute to theft of trade secrets by foreign actors.[108] In the Senate, the EEA emerged from the Select Committee on Intelligence and the Judiciary Subcommittee on Terrorism, Technology, and Government Information. In the House, it came out of the Judiciary Subcommittee on Crime.[109] The prohibition on industrial espionage became Section 1831[110] of the Act, which covers theft of trade secrets to benefit a "foreign government, foreign instrumentality or foreign agent."

Before Congress passed the EEA, however, it added a provision that applied to domestic trade secret theft, Section 1832. One of the main reasons for the expansion of the EEA to domestic trade secret theft cases–which are far more common than theft by foreign ones[111]–was concern that a foreign-only law would violate international trade treaties.[112] Congress spent little time thinking through how Section 1832 would interact with existing intellectual property laws. There was no substantive discussion of intellectual property issues in the committee reports or the floor debates, nor did Congress hear any testimony from intellectual property experts or practitioners.[113] Nothing in the

103. Pub. L. No. 102-561, 106 Stat. 4233 (codified as amended at 18 U.S.C. § 2319 (2006)).

104. Pub. L. No. 104-153, 110 Stat. 1386 (1996).

105. Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C., 28 U.S.C. § 4001 (2006)).

106. Pooley et al., *supra* note 78, at 178.

107. Pub. L. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C. §§ 1831-39 (2006)).

108. POOLEY, *supra* note 18, § 13.03[1] (noting that the EEA bill "was amended during the legislative process to cover virtually all forms of misappropriation").

109. Dreyfuss, *supra* note 52, at 5.

110. *See* 18 U.S.C. § 1831 (2006).

111. *See* Pacini & Placid, *supra* note 17, at 102.

112. Pooley et al., *supra* note 78, at 187.

113. Craig L. Uhrich, *The Economic Espionage Act–Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 171 (2001).

legislative history suggests that Congress considered how to strike the correct balance between protecting private rights to information and ensuring that no more information was removed from the public domain than was necessary. On the contrary, the House and Senate committee reports and the floor debate demonstrated "the one-sided, pro-business nature of the EEA."[114]

The business community and prosecutors generally welcomed the EEA as the federal statutory tool that they had long wanted to deter and punish theft of trade secrets. The EEA made it a federal crime to convert a trade secret to one's own benefit, or to the benefit of another, intending or knowing that the act would injure the trade secret's rightful owner.

Criminal laws are often narrower than their civil analogues, but in a wide range of areas the EEA pushed theft of trade secrets further than the civil–and even state criminal–laws had. Not surprisingly, the Act expressly eliminated the problem that had emerged with the NSPA. Rather than restrict itself to physical goods, the Act covered information "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[115]

But the EEA's broadened definition went beyond questions of form. It took a more expansive view of what kind of information could qualify as a trade secret.[116] State criminal statutes often defined trade secrets as "scientific or technical information," but the EEA adopted a variation on the UTSA's definition, including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes."[117] This definition drew within it a wide range of mundane business information, including advertising plans, customer lists, and personnel information.

The EEA also took a liberal view of the reference point for determining whether information had effectively been kept secret.[118] At state law, the issue was generally what a business's competitors knew about the information.[119] In the EEA, the relevant question was whether information was not "generally known to" or not "readily ascertainable" by "the public."[120] This was a significant alteration, because insiders in a business are considerably more likely to know about particular processes and methods than is the public.[121]

The EEA was also expansive in its definition of what constituted misappropriation. The Act made it illegal to "appropriate[]" or "take[]" a trade

114. Simpson, *supra* note 39, at 1148.
115. 18 U.S.C. § 1839(3) (2006).
116. POOLEY, *supra* note 18, § 13.03[2].
117. 18 U.S.C. § 1839(3) (2006).
118. Pooley et al., *supra* note 78, at 199.
119. *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 438 (1990).
120. 18 U.S.C. § 1839(3)(B) (2006).
121. *See* Moohr, *supra* note 71, at 917.

secret without the owner's authorization.[122] That language would appear to include not just taking information by "inappropriate" means, but taking it by means that are generally permitted by civil trade secret laws, such as by looking at a competitor's operation from across the street.[123] The EEA also arguably made it illegal for someone to make off with a trade secret through memorization. The Act did not expressly state that theft of a trade secret by committing it to memory was illegal, but by including in the definition one who "communicates" or "conveys" information,[124] without any requirement that they copy or download it, the statute strongly suggested that no physical item or digital record had to be taken. Most states do not criminalize theft of trade secrets through memorization.[125]

The EEA may also have broadened trade secret law in another important respect by arguably prohibiting reverse engineering.[126] Reverse engineering is the act of "starting with [a] known product and working backward to divine the process which aided in its development or manufacture."[127] Intellectual property regimes generally permit reverse engineering, seeing it not as an infringement but rather as a method of promoting innovation, and the trade secret laws of all states allow it.[128]

The EEA does not directly state that reverse engineering can be a form of trade secret theft. But the failure of the EEA to expressly include protection for it has been called "troubling."[129] The Act's pronounced ambiguity on the question, which has been widely commented upon in the academic literature,[130] should give pause to anyone who is considering undertaking a reverse engineering effort. That is particularly the case given the substantial criminal penalties that could be imposed.

The EEA is also expansive in its criminalization of acts falling short of actual theft of trade secrets. Given that it was extending federal criminal law to an area that it had not occupied before, Congress could have focused the Act on the most clear-cut instances of actual theft. Instead, the EEA was written to cover any third party who "receives, buys, or possesses such information" knowing that it was "stolen or appropriated, obtained, or converted without

---

122. 18 U.S.C. § 1832(a)(1) (2006).

123. *See* Pooley et al., *supra* note 78, at 192-93.

124. 18 U.S.C. § 1832(a)(2) (2006).

125. Moohr, *supra* note 71, at 876.

126. *See* Dreyfuss, *supra* note 52, at 15; Pooley et al., *supra* note 78, at 195.

127. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); *see also* Pooley et al., *supra* note 78, at 195-96.

128. Uhrich, *supra* note 113, at 167 & n.160.

129. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1578 & n.6 (2002).

130. *See, e.g.*, Pooley et al., *supra* note 78, at 195; Samuelson & Scotchmer, *supra* note 129, at 1577.

authorization."[131] It also makes it a crime to attempt or conspire to commit any of the prohibited actions.[132]

There was one more way in which the EEA was notably tough: it carried heavy criminal sanctions. Penalties for violating the act range up to ten years in prison, along with fines that can reach five million dollars. These penalties significantly exceed those for other forms of intellectual property misappropriation. Criminal copyright infringement carries a maximum five-year prison sentence, and patent infringement is not a crime at all.[133]

Broad as the EEA was, it did include a provision that significantly limited its scope: an interstate commerce requirement. To be covered by the Act, the trade secret that was taken had to be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[134] This condition was not contained in the UTSA, and Congress did not include it in Section 1831 of the EEA. Given that the EEA was enacted shortly after the Supreme Court raised the bar on Congress's ability to legislate under the Commerce Clause,[135] this provision may have been added to help the law survive judicial review.[136]

Commentators have criticized the interstate commerce requirement as "strange" and "unnecessary."[137] It was unnecessary because it excluded more trade secrets from the statute's reach than the Supreme Court's Commerce Clause jurisprudence required.[138] It was strange because it interfered with important areas of coverage, areas about which Congress appeared to be particularly concerned.

II. The Holes in the Economic Espionage Act

It has long been known that the federal criminal law of trade secrets contains gaps. Prosecutors who tried to use the NSPA have been on notice for decades that they might lose their case if the theft at issue involved an intangible item, such as a computer source code.[139] Indeed, Congress was motivated to enact a new law, the EEA, in part due to its awareness that the NSPA could not be counted on to reach this significant category of information.[140]

---

131. 18 U.S.C. § 1832(a)(3) (2006).
132. 18 U.S.C. § 1832(a)(4)-(5) (2006).
133. Moohr, *supra* note 71, at 863.
134. 18 U.S.C. § 1832(a) (2006).
135. *See infra* Section III.A.
136. *See infra* Section III.A; *see also* POOLEY, *supra* note 18, § 13.03[3].
137. POOLEY, *supra* note 18, § 13.03[3]; *see also* Pooley et al., *supra* note 78, at 200-01.
138. *See infra* notes 188-189, 245-251 and accompanying text.
139. *See, e.g.*, United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991); United States v. Kwan, No. 02 CR. 241(DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003).
140. *See* Coblenz, *supra* note 79, at 310 n.394 (citing H.R. REP. NO. 104-788, at 6 (1996)).

The EEA's gaps were also known, or at least strongly suspected. Commentators had warned that the Act's interstate commerce language carved out from coverage a significant number of trade secrets that were not related to or included in a product intended for interstate commerce, including important information that companies intended to keep for internal use.[141] A court might find that trade secrets that merely in some way affected interstate commerce were covered by the EEA,[142] but commentators warned that they might not be.[143]

Although the weaknesses of federal trade secret law were known, the Second Circuit's *Aleynikov* ruling was jolting. The three-judge panel, in a unanimous decision, made the strongest case yet that the EEA's interstate commerce language excluded from coverage a swath of trade secrets. It also became clear once the ruling came down just how much important commercial information fell within this excluded category.

A. United States v. Aleynikov

In the sometimes-gray world of trade secrets, Sergey Aleynikov was a defendant who evoked little sympathy. Aleynikov was a well-compensated computer programmer for Goldman Sachs who helped develop the computer code for the firm's HFT system. Goldman kept the HFT system for its own use and did not license it to anyone. The system was of considerable value to Goldman, and it went to great lengths to protect its secrecy so competitors could not take advantage of it. The firm had policies that required Aleynikov to keep the system's source code confidential.[144]

Aleynikov later accepted a job at a rival company that paid over $1 million a year, nearly three times his Goldman salary. Teza Technologies LLC, a Chicago-based investment firm, had hired him to help it develop its own HFT system.[145] Teza's founder informed Aleynikov that he expected Aleynikov to help the firm develop a trading system within six months, although evidence at trial showed that it would take twenty programmers approximately two years to create a similar HFT system from scratch.[146]

On his last day of work, June 5, 2009, right before his departure party, Aleynikov encrypted more than 500,000 lines of source code for Goldman's HFT system and uploaded them to a server in Germany.[147] Aleynikov erased records of the encryption and the transfer and later, when he arrived at home,

---

141. *See, e.g.*, POOLEY, *supra* note 18, § 13.03[3].

142. *See, e.g.*, United States v. Aleynikov, 785 F. Supp. 2d 46, 60-61 (S.D.N.Y. 2011), *rev'd*, 676 F.3d 71 (2d. Cir 2012).

143. *See, e.g.*, POOLEY, *supra* note 18, § 13.03[3].

144. United States v. Aleynikov, 676 F.3d 71, 74 (2d Cir. 2012).

145. Brief for the United States of America at 6-7, *Aleynikov*, 676 F.3d 71 (No. 11-1126).

146. *Id.* at 7.

147. *Aleynikov*, 676 F.3d at 74.

downloaded the source code from the German server to his home computer.[148] Aleynikov flew to Chicago a few weeks later to meet with officials at Teza. He brought portions of Goldman's HFT source code with him on a flash drive and a laptop computer.[149]

When Aleynikov returned home he was arrested at the airport. Federal prosecutors charged him with theft of trade secrets under the NSPA, the EEA, and the Computer Fraud and Abuse Act,[150] although the computer fraud count was dismissed from the indictment.[151] A jury of the U.S. District Court for the Southern District of New York convicted him on both the NSPA and EEA counts, and he was sentenced to 97 months of imprisonment, supervised release, and a fine.[152]

In his appeal, Aleynikov argued that his actions did not properly fall under either the NSPA or the EEA. He could not be convicted under the NSPA, he maintained, because the computer code that he stole was "intangible property" that was not "goods, wares, or merchandise" under the terms of the statute.[153] Aleynikov argued that his actions were not covered by the EEA because the code was not "a product that is produced for or placed in interstate or foreign commerce."[154]

The Second Circuit agreed on both counts. On February 16, 2012, after hearing oral arguments in the appeal, the court abruptly ordered that Aleynikov be released.[155] In April, the three-judge panel issued a unanimous written decision.[156] On the NSPA charge, it ruled that the government had failed to prove that Aleynikov had stolen "goods, wares [or] merchandise."[157]

The Second Circuit noted that as far back as 1966, it had resisted applying the NSPA to the theft of intellectual property. In *United States v. Bottone*,[158] the Second Circuit upheld a conviction under the NSPA for transporting across

148. Brief for the United States of America, *supra* note 145, at 8.

149. *Aleynikov*, 676 F.3d at 74.

150. 18 U.S.C. § 1030 (2006).

151. The district court ruled that because Aleynikov was authorized to access Goldman's computer system he did not violate the Act, which requires unauthorized use of a computer. *See* United States v. Aleynikov, 737 F. Supp. 2d 173, 191-94 (S.D.N.Y. 2010).

152. *Aleynikov*, 676 F.3d at 75.

153. Brief for Defendant-Appellant, *supra* note 24, at 14-20.

154. *Id.* at 24-30.

155. United States v. Aleynikov, No. 11-1126, 2012 WL 591980, at *1 (2d Cir. Feb. 17, 2012), *rev'g* 785 F. Supp. 2d 46 (S.D.N.Y. 2011) (amended order reversing the judgment of conviction and remanding the matter to the district court to release Aleynikov on bail pending the Second Circuit's Opinion); Peter Lattman, *Government Dealt Setback in Case Against Ex-Goldman Programmer*, N.Y. TIMES (Feb. 17, 2012, 9:43 PM), http://dealbook.nytimes.com/2012/02/17/justice-dealt-setback-in-case-against-ex-goldman-programmer.

156. *Aleynikov*, 676 F.3d 71, *rev'g* 785 F. Supp. 2d 46 (S.D.N.Y. 2011); Michael J. De La Merced and Peter Lattman, *Appeals Court Limits Law Used in Goldman Programmer Case*, N.Y. TIMES (Apr. 11, 2012, 11:00 AM), http://dealbook.nytimes.com/2012/04/11/court-limits-scope-of-corporate-espionage-laws-in-goldman-programmer-case.

157. *Aleynikov*, 676 F.3d at 76.

158. 365 F.2d 389 (2d Cir. 1966).

state lines photocopied documents that contained manufacturing processes for pharmaceuticals. The *Bottone* Court emphasized that the photocopies counted as tangible goods under the NSPA. It went on to say that had there been no photocopies–if "a carefully guarded secret formula was memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed"–the "tangible property" requirement of the statute would not have been met.[159]

The *Aleynikov* Court noted that the Supreme Court had reached a similar conclusion in *Dowling*.[160] In *Dowling*, the Court ruled that "the NSPA did not apply to an interstate bootleg record operation."[161] The government had charged the defendants with violating the NSPA by making unauthorized copies of copyrighted music and transporting the recordings across state lines. The Court, however, ruled that the NSPA did not apply because the misappropriated music was not "stolen, converted or taken by fraud" within the meaning of the statute.[162] The copyright holders' rights may have been infringed but that was not the sort of theft the NSPA contemplated. The key, the Court said, was that there must be "a physical identity between the items unlawfully obtained and those eventually transported."[163] Taking a copy while the original remains in the possession of the owner does not qualify.[164] The *Aleynikov* Court said that by the same logic, Aleynikov's theft did not violate the NSPA because he was not accused of "physically seiz[ing] anything tangible from Goldman, such as a compact disc or a thumb drive."[165] In the Second Circuit's reading, *Dowling* stands for the proposition that "theft and subsequent interstate transmission of purely intangible property is beyond the scope of the NSPA."[166]

On the EEA charge, the Second Circuit also found that Aleynikov's actions had not violated the law. The *Aleynikov* Court noted that Section 1832 covered only trade secrets "related to or included in a product that is produced for or placed in interstate or foreign commerce."[167] This language, the Second Circuit observed, did not appear in Section 1831, the provision that applies to foreign espionage.[168] "The words of limitation in Section 1832," the *Aleynikov* Court concluded, "were deliberately chosen."[169] They must "be read as a term of limitation."[170]

---

159. *Id.* at 393.
160. 473 U.S. 207 (1985); *see supra* notes 87-92 and accompanying text.
161. *Aleynikov*, 676 F.3d at 77.
162. *Dowling*, 473 U.S. at 216.
163. *Id.*
164. *See id.* at 216-18.
165. *Aleynikov*, 676 F.3d at 78.
166. *Id.* at 77.
167. *Id.* at 79.
168. *Id.*
169. *Id.* at 80.
170. *Id.* at 79.

The Second Circuit said that the "natural reading" of the language would have to take into account the meaning of each of the paired phrases. Products that have been "'placed in' commerce have already been introduced into the stream of commerce and have reached the marketplace."[171] Products that are "produced for" commerce, the Second Circuit said, were ones that "are still being developed or readied for marketplace."[172]

The district court in the *Aleynikov* case had adopted a more expansive interpretation of the interstate commerce language. It concluded that the source code that Aleynikov stole had been "'produced for' interstate commerce because 'the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the Trading System was to engage in interstate and foreign commerce,'" and it noted "the Trading System generates many millions of dollars in annual profits."[173]

The *Aleynikov* Court regarded the district court's interpretation as flawed. The Second Circuit said that the district court made the mistake of trying to understand the phrase "produced for . . . interstate or foreign commerce" by examining it "in a vacuum."[174] It is a basic canon of statutory construction, the court noted, that the words of a statute must be read in the context of the overall statutory scheme, with due consideration to the words around them. In interpreting the operative language, the court said, the phrase "produced for" can only be properly understood in conjunction with its paired phrase, "placed in." If "produced for" had the broad meaning the district court assumed–and it covered the HFT system code–there would be no need for the "placed in" language, since anything "placed in" interstate commerce would be "produced for" it as well. In that case, the phrase "placed in" would be "surplusage," unnecessary because other words already convey the meaning ascribed to it. The canons of statutory construction instruct that courts should, if possible, avoid surplusage and strive to give meaning to every part of a statute.[175]

The Second Circuit ended its analysis by stating that if Congress had intended to give Section 1832 the broad sweep that the government and the district court wanted to read into it, Congress could have employed the sort of language that indicates an intention to invoke Congress's full regulatory power under the Commerce Clause. The Supreme Court had explained in *United States v. Lopez*[176] that Congress's power extends to activities that "substantially affect interstate commerce" and no further.[177] If Congress had wanted to sweep

171. *Id.* at 80.
172. *Id.*
173. *Id.* (*quoting* United States v. Aleynikov, 737 F. Supp. 2d 173, 179 (S.D.N.Y. 2010)).
174. *Id.* (*quoting* Davis v. Mich. Dep't of Treasury, 489 U.S. 803, 809 (1989)).
175. *Id.* at 80-81.
176. 514 U.S. 549 (1995).
177. *Id.* at 558-59.

in actions like Aleynikov's, the court said, it should have used the sort of broad language that the *Lopez* ruling set out.

Once the interstate commerce provision of Section 1832 is given its proper interpretation, the Second Circuit said, it is clear that Aleynikov's theft of Goldman's HFT source code does not fall under the statute. Goldman had "no intention of selling its HFT system or licensing it to anyone," the court noted. To the contrary, Goldman went to great lengths to keep the system secret since its enormous profitability depended in large part on competitors not having access to it. Because the HFT was never intended to enter into or pass in interstate commerce or to make anything that does, the court said Aleynikov's actions were "not an offense under the EEA."[178]

Based on the Second Circuit's interpretation of the statutes, Aleynikov came very close to committing a crime–and the fact that he did not was likely due to mere chance. Aleynikov was not in danger under the NSPA, because the thing he stole–the HFT source code–was not covered under the statute. But if he had taken the smallest physical object at the time of his theft, he would have violated the NSPA. If he had taken the source code on a Goldman laptop computer, or downloaded it to a computer disk, or if he had even merely taken notes on Goldman paper and taken them with him, Aleynikov's conduct would likely have fallen under the physicality requirement of the NSPA. It makes little sense to have criminal culpability ride on whether a multi-million-dollar theft of trade secrets was carried out by theft of an inexpensive computer disk, but that is what the law apparently requires.[179]

The Second Circuit's interpretation of the NSPA and its ruling that Aleynikov did not run afoul of it are almost certainly correct. The government tried to bring the stolen source code under the statute, but the court convincingly explained why it did not fit given the NSPA's text and legislative history. Moreover, the legislative history of the EEA provides additional support for the court's conclusion. When Congress enacted the EEA, a House report accompanying the bill stated that the new law was needed because "courts have been reluctant to extend the reach of" the NSPA to cover intellectual property.[180]

Supreme Court precedent further supports the Second Circuit's conclusions. Although *Dowling* was not a case about computer technology, the Supreme Court's analysis strongly suggests that duplicating computer code and absconding with the copied information does not qualify as theft under the NSPA. The weight of authority from other circuits is also in line with the Second Circuit's holding. The U.S. Court of Appeals for the Tenth Circuit, in *United States v. Brown*, ruled that stolen computer code, as "intangible

178. *Aleynikov*, 676 F.3d at 82.

179. *See* Pooley et al., *supra* note 78, at 186; *see also infra* notes 206-208 and accompanying text.

180. *See* H.R. REP. NO. 104-788, at 6 (1996).

intellectual property," could not be the sort of "goods, wares, [or] merchandise" covered by the NSPA.[181] In a 2011 case, the U.S. Court of Appeals for the Sixth Circuit similarly concluded that electronically stored information, being intangible, does not fall under the NSPA.[182] In a low-technology case involving theft of "Comdata codes"–a series of numbers that truck drivers used to acquire cash while on the road by writing them down and cashing them like a check–the U.S. Court of Appeals for the Seventh Circuit found that the NSPA did not apply.[183]

The government argued that the Second Circuit's ruling in *Bottone* supported its more expansive reading of the NSPA. In the government's view, Aleynikov's saving the source code to his laptop and flash drive was comparable to Bottone's photocopying of trade secrets. As Judge Friendly wrote for the *Bottone* panel, a defendant should not escape criminal liability because "the intangible information that was the purpose of the theft was transformed and embodied in a different physical object."[184] The government was right to press this point, since saving the source code to a computer falls somewhere between the memorization of trade secrets that the *Bottone* Court said would clearly not fall under the NSPA and the taking of photocopies, which the court ruled was covered. In the end, however, what mattered in *Bottone* was whether the defendant had taken a stolen tangible good across state lines. A photocopy of secret formulas clearly meets that standard. In the case of Aleynikov's laptop, there was no stolen tangible good–just copied bits of information in storage in his own computer's memory.

The Second Circuit's ruling on the EEA count also appears to be well founded, although there are ways in which the court should have explained its position more fully. The panel's argument that the district court's interpretation of the "produced for" and "placed in" language created surplusage is ultimately persuasive, but the court should have acknowledged that the interpretation it argues for creates surplusage issues as well.[185]

---

181. United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991).

182. *See* United States v. Batti, 631 F.3d 371, 376-77 (6th Cir. 2011); *see also* United States v. Martin, 228 F.3d 1, 13 (1st Cir. 2000) (ruling that "purely intellectual" property does not fall under the NSPA).

183. *See* United States v. Stafford, 136 F.3d 1109, 1114-15 (7th Cir. 1998).

184. United States v. Bottone, 365 F.2d 389, 393-94 (2d Cir. 1966).

185. The Second Circuit could also have been less emphatic about the need to avoid surplusage in criminal statutes. In fact, criminal statutes not infrequently contain overlapping provisions. *See, e.g.*, 18 U.S.C. § 1343 (2006) ("Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . ."); 18 U.S.C. § 1344 (2006) ("Whoever knowingly executes, or attempts to execute, a scheme or artifice-(1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises . . . .").

The *Aleynikov* Court sets up a dichotomy in which products "placed in" interstate commerce are ones that have already been put in the stream of commerce and reached the marketplace, while ones "produced for" are still being readied for the marketplace. But using these definitions, it might be argued that the "placed in" provision is surplusage because any product "placed in" interstate commerce has presumably been "produced for" interstate commerce. Are there really products that a firm places in interstate commerce that it did not produce for interstate commerce?

In fact, there may well be. If Goldman had decided to start selling its proprietary HFT code to other investment firms, a defendant charged with stealing it could protest–if the "placed in" language were not in the statute–that the thing he was accused of stealing had not in fact been "produced for" interstate commerce. It had, rather, simply ended up there eventually. It is not unreasonable, given Congress's expressed intention to "provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets,"[186] for it to have wanted to be sure that the law covered two distinct categories: (1) products produced for interstate commerce that have not yet been placed in it; and (2) products placed in interstate commerce, whether or not the original intention had been to produce them for it.

Another weakness of the Second Circuit's ruling on the EEA charge is its failure to fully engage the ways in which the HFT system source code might be seen as having entered interstate commerce. Goldman acquired some of the components of the code when it bought out Chicago-based Hull Trading in 1999 for $500 million and brought it to New York.[187] The code itself communicates with servers located in other states and other countries. It could be argued that the part of the code that Goldman acquired from Hull Trading was "placed in" interstate commerce, and the part that was not was "produced for" it.

Had the *Aleynikov* Court addressed these facts more directly, it could have made a strong argument that despite these interstate movements the code was neither "placed in" nor "produced for" interstate commerce. It might have been true that some of the code's component parts were in commerce, but the final product that they were subsumed in never was. Many things that are not produced for or placed in interstate commerce are made up of raw materials that were. If the origins of a product's component parts are enough to meet the interstate commerce test, there are few items–other than things grown locally or dug out of the ground–that would not qualify. As for the fact that the code itself communicates with servers in other states, that is evidence that the code affects

186. United States v. Yang, 281 F.3d 534, 543 (6th Cir. 2002); *see also* United States v. Tykarsky, 446 F.3d 458, 467 (3d Cir. 2006) ("[T]he Economic Espionage Act provides a 'comprehensive' solution for corporate espionage . . . .").

187. United States v. Aleynikov, 785 F. Supp. 2d 46, 51 (S.D.N.Y. 2011).

interstate commerce. It does not, however, mean that the code was placed in or produced for interstate commerce.

The Second Circuit provides several other strong bases for its conclusions about the EEA. It rightly notes that the Supreme Court has drawn a distinction between statutes in which Congress invokes its full power to regulate under the Commerce Clause and those in which it does not. When Congress uses the term "affecting . . . commerce" without any qualifications, the Supreme Court has stated, it is signaling its "intent to invoke its full authority under the Commerce Clause."[188] The more constrained language of the EEA, with its focus on whether the material was produced for or placed in interstate commerce, indicates that Congress did not intend to exercise its power up to its full constitutional authority.[189]

Other influential interpreters of this provision of the EEA have reached similar conclusions. The Department of Justice has advised in its internal manuals that "technical skills" are only a product that is produced for or placed in interstate commerce when they are contained in "a saleable, transportable good."[190] When the Department of Labor promulgated regulations under a portion of the Fair Labor Standards Act with parallel wording–"the production of goods for interstate commerce"–its interpretation resembled that of the Second Circuit. In 29 C.F.R. § 776.21(a), the Department stated that goods are produced for interstate commerce "where the employer intends, hopes, expects, or has reason to believe that the goods or an unsegregated part of them will move . . . in such interstate or foreign commerce."[191]

There is a final compelling reason that the Second Circuit's interpretation of the EEA is likely to prevail: the rule of strict construction of criminal statutes. When the Supreme Court invoked this principle in 1820 it was already an old rule, "perhaps not much less old than construction itself."[192] As the Court said more recently, "when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite."[193] The text of a criminal law forms a "linguistic wall," and it "will not be interpreted more broadly than the[] language reasonably permits, even if the legislature may have intended to criminalize

188. Jones v. United States, 529 U.S. 848, 854 (2000).

189. *Aleynikov*, 676 F.3d at 81-82.

190. Computer Crime and Intellectual Property Section, *Prosecuting Intellectual Property Crimes*, U.S. DEP'T OF JUSTICE 161 (3d ed. 2006), *archived by* 5th Cir. Library, http://www.lb5.uscourts.gov/ArchivedURLs/Files/09-20074%281%29.pdf (Apr. 30, 2010).

191. *See* Kim v. Park, No. 08 C 5499, 2009 WL 1702972, at *4 (N.D. Ill. June 16, 2009) (quoting 29 C.F.R. § 776.21(a) (2007)).

192. Dowling v. United States, 473 U.S. 207, 213 (1985) (quoting United States v. Wiltberger, 5 Wheat. 76, 95 (1820)).

193. United States v. Universal C.I.T. Credit Corp., 344 U.S. 218, 221-22 (1952).

additional conduct."[194] If Congress wanted to punish theft of items like Goldman's computer code that were not in interstate commerce and were never intended to be, it needed to do so in language that puts people on notice of precisely what actions are illegal.

With its ruling, the Second Circuit effectively insulated Aleynikov's actions, and a wide swath of other kinds of theft, from federal criminal law. In his concurring opinion, Judge Calabresi attempted to chart a path forward. Although he agreed that the statute as written did not cover Aleynikov's actions, he also said he found it hard to believe that Congress meant to exempt the sort of behavior Aleynikov had engaged in. Judge Calabresi expressed his "hope that Congress will return to the issue and state in appropriate language" what it was they "meant to make criminal."[195]

B. Unprotected Digital Trade Secrets

The interpretation of the EEA that the Second Circuit adopted in *Aleynikov* leaves sizeable holes in the law of trade secrets.[196] If the EEA criminalizes only theft of trade secrets that are "related to or included in a product that is produced for or placed in interstate or foreign commerce," and that phrase means what the Second Circuit panel says it does, it does not reach a great deal of intellectual property owned and used by American companies.

In this digital age, computer codes and other technological formulas and instructions are of growing significance, and are "often at the core of a company's business engine."[197] Computer software is especially vulnerable to those seeking to steal trade secrets. Computer programs are "extremely portable" and easily used by competitor firms. Programs that are enormously expensive to develop "can be copied for a small fraction of the development costs."[198]

---

194. LAWRENCE M. SOLAN, THE LANGUAGE OF STATUTES: LAWS AND THEIR INTERPRETATION 42 (2010).

195. United States v. Aleynikov, 676 F.3d 71, 83 (2d Cir. 2012) (Calabresi, J., concurring).

196. This weakening of trade secret law comes at a time when the U.S. Attorney for the Southern District of New York, Preet Bharara, has made a point of emphasizing the need to combat cybercrime. *See, e.g.*, Azam Ahmed & Peter Lattman, *Victory Spurs Talk on Bharara's Next Move*, N.Y TIMES, June 15, 2012, http://dealbook.nytimes.com/2012/06/15/victory-spurs-speculation-on-bhararas-next-move (quoting Bharara as saying that "of all the issues I face as United States Attorney . . . cyberthreat in all of its breadth, variety and complexity is what worries me the most . . . ."); *see also* Preet Bharara, Op-Ed., *Asleep at the Laptop*, N.Y. TIMES, June 3, 2012, http://www.nytimes.com/2012/06/04/opinion/preventing-a-cybercrime-wave.html (emphasizing the importance of "the gathering cyberthreat").

197. Eric Friedberg, James Aquilina & Matt Friedrich, *Investigating Source Code Thefts for Presentation at the 24th Annual National Institute on White Collar Crime*, STROZ FRIEDBERG, 1 (Feb 24-26, 2010), http://www.strozfriedberg.com/files/Publication/afba300e-1c3e-4007-8dc6-2aba5480aa87/Presentation/PublicationAttachment/74e59c67-99f0-407d-8626-316bdf6ac495/SourceCodeTheft.pdf.

198. 2 MELVIN F. JAGER, TRADE SECRETS LAW § 9:1 (Release No. 19 2012).

One major category of trade secrets that the *Aleynikov* ruling leaves unprotected is the kind that was at issue in that case: computer codes used by the financial services industry. The industry increasingly relies on complex code to evaluate risk and carry out trades. Financial services firms are locked in an "algorithmic arms race."[199] These firms are developing and deploying complex computer formulas that draw on vast quantities of data including such variables as stock market momentum, interest rate fluctuations, and global weather conditions.[200]

Hedge funds are increasingly trading algorithmically. By one estimate, eighty percent of hedge funds will be trading algorithmically within the next three years, joining the many quant funds that already do so. "Algorithms are changing the world of finance, for multi-asset trading, risk management, and cost analysis;" they are "the lifeblood of trading firms."[201]

With these firms under enormous pressure to produce market-beating returns, algorithms have become "business critical asset[s]" that are at considerable risk of theft.[202] These algorithms are tempting targets for economic espionage. Computer code is stored in a form that can readily be copied and transported, and easily misappropriated once it is taken. Code of this sort is often labor-intensive and expensive to develop, and because it can produce enormous monetary payoffs its value is clear to potential thieves. It can be sold for a sizeable bounty to a financial services firm, or the thieves can use the code to start a rival business. In another common scenario, a programmer can offer up the code to make himself more attractive to a prospective employer. In Aleynikov's case, his starting salary at Teza, where he arrived with Goldman's HFT system's source code in hand, was about $1.2 million, compared to the $400,000 he was making at Goldman.[203]

There have been a number of high-profile prosecutions recently involving theft of financial-services computer code. In April 2010, two months after Aleynikov's indictment, Samarth Agrawal, a trader at Société Générale in New York, was charged with stealing HFT software code from his employer. Like Aleynikov, he was accused of offering the code to another financial services firm where he had accepted a job.[204] Agrawal was convicted at trial, and he

199. Tommy Wilkes and Laurence Fletcher, *Special Report: The Algorithmic Arms Race*, REUTERS (May 21, 2012, 2:24 AM), http://www.reuters.com/article/2012/05/21/us-trading-blackbox-idUSBRE84K07320120521.

200. *Id.*

201. Louis Lovas, *Breaking the Code Theft Brain Drain*, ADVANCED TRADING, June 15, 2012, http://www.advancedtrading.com/algorithms/breaking-the-code-theft-brain-drain/240002167.

202. *Id.*

203. *Id.*; *see supra* note 145 and accompanying text.

204. Bob Van Voris, *SocGen Ex-Trader Agrawal Sentenced for Software Theft*, BLOOMBERG (Mar. 1, 2011, 6:11 AM), http://www.bloomberg.com/news/2011-02-28/ex-societe-generale-trader-gets-3-years-in-prison-for-theft-1-.html. Agrawal was convicted of theft of trade secrets and, in March 2011, was sentenced to three years in prison. *Id.*

appealed while beginning to serve his 36 month prison sentence.[205] Unlike Aleynikov, Agrawal printed out the HFT code that he took on paper belonging to his employer, which created a tangible piece of property, and that fact could make all the difference in bringing his theft under the NSPA.[206]

In October 2011, Yihao "Ben" Pu, a former software engineer at Citadel Investment Group, was indicted on charges of stealing that firm's HFT code, which operated one of the most sophisticated trading systems in the financial sector.[207] Pu was accused of uploading code to his personal devices and then attempting to destroy the evidence.[208] Like the Goldman HFT source code, the code stolen by Pu was being used by the hedge fund for internal use. There was another similarity between the Pu and Aleynikov cases: Citadel claimed that Pu was speaking with a recruiter at Teza Technologies, the same firm to which Aleynikov brought his stolen code. The founder of Teza had been sued by Citadel for breach of contract, and as part of that suit he was ordered to pay a sizeable financial penalty for destroying information contained on a home computer.[209]

Another case of source code theft involved the Federal Reserve Bank of New York's Government-Wide Accounting and Reporting Program. In May 2010, Bo Zhang–a computer programmer who worked for a contractor employed by the bank–pled guilty to copying computer code that kept track of billions of dollars of transfers of funds between government agencies. Zhang was able to steal the code simply by copying the code onto the hard drive of a computer in his office and then transferring it to an external hard drive, which he brought home with him.[210]

A second category of trade secrets made vulnerable by the *Aleynikov* ruling is the source codes of technology companies. For technology companies,

---

205. Basil Katz, *Ex-SocGen Trader: Taking of Bank Code Not a Crime*, REUTERS (June 21, 2012, 2:44 AM), http://in.reuters.com/article/2012/06/21/socgen-agrawal-idINL1E8HJ5RK20120621.

206. If the act of printing the stolen code on paper instead of uploading the code to a German server marks the difference between a conviction and an acquittal under the NSPA, the arbitrariness of the distinction points toward revising the NSPA as well as the EEA. *See* Jennifer L. Achilles, *Where Two Bank Employees Steal Proprietary Trading Code, Could One Stay in Jail Merely Because He Printed It Out First?*, REED SMITH: GLOBAL REGULATORY ENFORCEMENT LAW BLOG (June 29, 2012), http://www.globalregulatoryenforcementlawblog.com/2012/06/articles/government-investigations/where-two-bank-employees-steal-proprietary-trading-code-could-one-stay-in-jail-merely-because-he-printed-it-out-first/.

207. Azam Ahmed, *Ex-Citadel Employee Charged With Stealing Trade Secrets*, N.Y. TIMES (Oct. 13, 2011, 5:03 PM), http://dealbook.nytimes.com/2011/10/13/ex-citadel-employee-charged-with-stealing-trade-secrets.

208. *Id.*

209. Azam Ahmed, *Court Grants Citadel Restraining Order Against Employee*, N.Y. TIMES (Aug. 30, 2011, 5:29 PM), http://dealbook.nytimes.com/2011/08/30/court-grants-citadel-restraining-order-against-employee.

210. Patricia Hurtado, *Programmer Charged with Stealing U.S. Treasury Software from New York Fed*, BLOOMBERG (Jan. 19, 2012, 3:10 AM), http://www.bloomberg.com/news/2012-01-18/man-said-to-be-charged-by-u-s-in-federal-government-computer-data-theft.html; Basil Katz, *Chinese Man Pleads Guilty to NY Fed Cyber Theft*, REUTERS (May 29, 2012, 6:30 PM), http://www.reuters.com/article/2012/05/29/us-usa-crime-fed-idUSBRE84S1FI20120529.

the computer codes that control their critical functions are among their most valuable assets. If they are stolen, rivals can quickly and inexpensively replicate the company's services and compete for users. Thefts of this kind appear to be occurring with some frequency. The vice president of threat research of McAfee, a cybersecurity firm, has said: "Companies . . . are getting raped and pillaged every day. They are losing economic advantage and national secrets to unscrupulous competitors. . . . This is the biggest transfer of wealth in terms of intellectual property in history. . . . The scale at which this is occurring is really, really frightening."[211]

It is difficult to know precisely how much damage is being done by the theft of technology company source codes. A technology company whose code is stolen has strong reasons for not divulging the theft, ranging from the impact on its brand to the possible effect on its stock price.[212] There have, however, been a number of major thefts of technology company source codes that have become public, and they suggest the magnitude of the problem. In December 2009, hackers carried out a major attack on Google aimed at stealing its source code–an attack that was described as an attempt to steal Google's "crown jewels."[213] The hackers gained access to Google's network by sending e-mails to employees with malicious PDF attachments that installed a backdoor Trojan horse.[214] The attackers reportedly succeeded in stealing the code for Google's Gaia program, the password system that controlled access to Google services by millions of users around the world.[215] It was later revealed that the same hack attack also targeted 33 other companies, including the software maker Adobe, defense contractors, and financial institutions.[216]

The Google attack was a "highly sophisticated" hack originating in China,[217] but hacks need not be sophisticated to wrest away immensely valuable trade secrets. In April 2011, a hacker operating out of his bedroom in his parents' home in England was able to break into Facebook's computer system and steal its source code, which has been described as "arguably the

211. Jim Finkle, *"State Actor" Behind Slew of Cyber Attacks*, REUTERS (Aug. 3, 2011, 7:17 PM), http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803.

212. Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25, 29 & n.36 (2001).

213. Kim Zetter, *Report: Google Hackers Stole Source Code of Global Password System*, WIRED: THREAT LEVEL (Apr. 20, 2010, 1:06 PM), http://www.wired.com/threatlevel/2010/04/google-hackers.

214. Kim Zetter, *Google Hackers Targeted Source Code of More than 30 Companies*, WIRED: THREAT LEVEL (Jan. 13 2010, 2:28 AM), http://www.wired.com/threatlevel/2010/01/google-hack-attack.

215. John Markoff, *Cyberattack on Google Said to Hit Password System*, N.Y. TIMES, Apr. 19, 2010, http://www.nytimes.com/2010/04/20/technology/20google.html.

216. Zetter, *Google Hackers Targeted Source Code of More than 30 Companies*, *supra* note 214.

217. Kim Zetter, *Google to Stop Censoring Search Results in China After Hack Attack*, WIRED: THREAT LEVEL (Jan. 12, 2010, 7:10 PM), http://www.wired.com/threatlevel/2010/01/google-censorship-china.

company's most valued and secret intellectual property."[218] The young man, who claimed he had no intention of profiting from the theft, pleaded guilty to unauthorized access to computer material and unauthorized modification of computer data. But the information would have been of considerable value to Facebook's social media competitors.[219]

Another area that the *Aleynikov* ruling leaves particularly vulnerable is R&D. Trade secret thieves often target corporate R&D programs, since they produce large amounts of valuable information that can be of use to other companies operating in the field or interested in entering it. In April 2012, the government filed charges against Xiaorong Wang for stealing trade secrets from Bridgestone Tire's Center for Research and Technology in Akron, Ohio.[220] The facility did research relating to an array of Bridgestone products, including rubber and tires.

Under the *Aleynikov* ruling, theft of trade secrets relating to specific products produced for or entered into interstate commerce is covered by the EEA. But a significant amount of corporate R&D is basic research, designed to make general advances in a field rather than to produce a particular product.[221] Microsoft, for example, runs Microsoft Research, which engages in "both basic and applied research without regard to product cycles."[222]

A trade secret law that fails to protect basic R&D is fundamentally flawed. Basic R&D is a bulwark of the economy. Although its benefits are difficult to precisely quantify, one study found that increases in research in the United States and four other developed countries may have been responsible for nearly fifty percent of U.S. economic growth between 1950 and 1993.[223] Although the EEA does not adequately cover basic R&D secrets, that omission was likely unintentional since "secret scientific research probably forms the great bulk of what Congress was trying to protect."[224]

---

218. Jeremy Kirk, *Facebook Hacker Comes Clean on "What Really Happened,"* PCWORLD, Apr. 26, 2012, http://www.pcworld.idg.com.au/article/422770/facebook_hacker_comes_clean_what_really_happened.

219. *See id.*

220. *See* Jim Mackinnon, *Akron-Based Bridgestone Americas Researcher Charged with Trade Secrets Theft*, OHIO.COM (Mar. 23, 2012, 1:05 AM), http://www.ohio.com/business/akron-based-bridgestone-americas-researcher-charged-with-trade-secrets-theft-1.284100; Press Release, U.S. Attorney's Office for the Northern District of Ohio, A Criminal Information Was Charging [sic] Xiaorong Wang, 50, of Hudson, Ohio, with Theft of Trade Secrets (Apr. 26, 2012), http://www.justice.gov/usao/ohn/news/2012/26AprilWang.html.

221. *See* WENDY H. SCHACHT, CONG. RESEARCH SERV., RL33528, INDUSTRIAL COMPETITIVENESS AND TECHNOLOGICAL ADVANCEMENT: DEBATE OVER GOVERNMENT POLICY 1-11 (2012), http://www.fas.org/sgp/crs/misc/RL33528.pdf.

222. *See Microsoft Research at a Glance*, MICROSOFT (May 2012), http://research.microsoft.com/en-us/press/overview.aspx (last visited Oct. 15, 2012).

223. Charles I. Jones, *Sources of U.S. Economic Growth in a World of Ideas*, 92 AM. ECON. REV. 220, 235 (2002).

224. POOLEY, *supra* note 18, § 13.03[3]. In addition to these areas that are closely tied to the emerging digital economy, the EEA as interpreted by the *Aleynikov* Court arguably does not apply to trade secrets about services, since they are not "products" produced for or entered into interstate

III. Toward an Economic Espionage Act 2.0

The normal state of affairs in business is free and robust competition, including the ability to take a competitor's methods and processes. Comment a of Section 757 of the Restatement (First) of Torts states: "The privilege to compete with others . . . includes a privilege to adopt their business methods, ideas or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition."[225] Trade secret law is a limitation on free competition based on the notion of "a public interest that is greater than the principle of free competition."[226]

The challenge faced by the EEA and other intellectual property laws is to impose limits on free competition that advance the public interest but do not go further. In the wake of the *Aleynikov* ruling, there were calls for Congress to amend the EEA.[227] The people urging these changes had a clear focus: filling the gap that the court had identified, which excluded from coverage computer code, pure research, and other information not related to or included in a product that is produced for or placed in interstate commerce. The way to do this would be to broaden the EEA's interstate commerce language.

In the commentary calling for the EEA to be amended, there was little discussion of the Act's other major flaw: its failure to consider the correct balance between how much information should be protected and how much should be left unprotected. The interstate commerce provision aside, the EEA is in important ways tilted in favor of those who hold trade secrets. In late 2012, the Senate took up Judge Calabresi's recommendation and passed a bill to amend the Act.[228] The bill is deficient, however, because it addresses the EEA's underinclusiveness–on the interstate commerce issue–but not the significant ways in which the Act is overinclusive.

A. Fixing the Interstate Commerce Provision

When Congress wrote the EEA, it does not appear to have deliberated greatly over the phrasing of the interstate commerce limitation of Section 1832. The language about the Act applying to a trade secret that is "included in a product that is produced for or placed in interstate or foreign commerce" comes from the House version of the bill. The "Section-by-Section" analysis of the

---

commerce. The effect of this is to "eliminate from coverage" of the Act "the fastest growing segment of the domestic economy." *Id.*

225. RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939); *see also* Symposium, *Panel III: Trade Secrets*, *supra* note 72, at 920 (comments of Prof. Sharon K. Sandeen) (quoting same).

226. Symposium, *Panel III: Trade Secrets*, *supra* note 72, at 920 (comments of Prof. Sharon K. Sandeen).

227. *See supra* notes 12-14 and accompanying text.

228. Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (as passed by Senate, Nov. 27, 2012).

House report on the EEA, however, makes no mention of the interstate commerce limitation and does not attempt to explain its wording.[229]

The timing of the law, however, suggests what Congress may have been thinking. The EEA was enacted one year after the Supreme Court decided *United States v. Lopez*,[230] the first new restriction on Congress's Commerce Clause authority since the New Deal. In *Lopez*, the Court struck down key portions of the Gun Free School Zones Act of 1990, which made it a federal crime "for any individual knowingly to possess a firearm at a place that the individual knows, or has reasonable cause to believe, is a school zone."[231] The Court emphasized that Congress's power to legislate under the Commerce Clause was limited. Reaching back to 1937, it quoted the Court's declaration in *NLRB v. Jones & Laughlin Steel Corp.*,[232] that congressional power "'may not be extended so as to embrace effects upon interstate commerce so indirect and remote that to embrace them, in view of our complex society, would effectively obliterate the distinction between what is national and what is local and create a completely centralized government.'"[233]

The *Lopez* Court decreed that for Congress to regulate an activity under its Commerce Clause authority, the activity had to "substantially affect" interstate commerce.[234] The Court stated that it had upheld congressional regulation of a wide array of activities that met this standard, ranging from coal mining[235] to hotels serving interstate guests,[236] to the production and consumption of homegrown wheat.[237] The Gun Free School Zones Act exceeded Congress's authority, the Court held, because the possession of a gun in a school zone does not substantially affect interstate commerce the way those other activities do.

When *Lopez* was decided, it was greeted as the beginning of a new era of federalism jurisprudence. In the popular press, the ruling was viewed as the harbinger of a "revolutionary states-rights movement within the Court."[238] The reception among legal scholars was not much more restrained. One constitutional law scholar, writing in the *Michigan Law Review*, hailed the *Lopez* ruling as "revolutionary and long overdue."[239]

---

229. *See* H.R. REP. NO. 104-788, at 10-14 (1996).

230. 514 U.S. 549 (1995).

231. 18 U.S.C. § 922(q)(1)(A) (Supp. V 1988).

232. 301 U.S. 1 (1937).

233. *Lopez*, 514 U.S. at 557 (quoting *Jones & Laughlin Steel Corp.*, 301 U.S. at 37).

234. *Id.* at 559.

235. *See, e.g.*, Hodel v. Virginia Surface Min. & Reclamation Ass'n, Inc., 452 U.S. 264 (1981).

236. Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241 (1964).

237. Wickard v. Filburn, 317 U.S. 111 (1942).

238. Timothy Phelps, *Judicial Revolution: Recent Cases Slant Towards States*, NEWSDAY, May 29, 1995, at A13.

239. Steven G. Calabresi, *"A Government of Limited and Enumerated Powers": In Defense of* United States v. Lopez, 94 MICH. L. REV. 752, 752 (1995).

It was not clear how far this revolution would go, but considering that the Supreme Court was willing to strike down a law that kept guns off school grounds, it appeared that it might go quite far. After *Lopez*, scholars and practitioners began to ask whether well-entrenched laws and regulations like the Clean Water Act, the Endangered Species Act, and the Migratory Bird Rule might be challenged under the Supreme Court's Commerce Clause revolution.[240] In 2000, in *United States v. Morrison*,[241] the Court showed that the principle it laid down in *Lopez* had enduring influence. The *Morrison* Court struck down part of the Violence Against Women Act of 1994,[242] ruling that Congress had exceeded its power under the Commerce Clause in passing it because "[g]ender-motivated crimes of violence are not, in any sense of the phrase, economic activity."[243]

Given the "temporal proximity between the enactment of the EEA and the decision in *Lopez*," it is not hard to imagine that Congress was looking to steer clear of any trouble with the Supreme Court over the Commerce Clause. The statutory phrasing that led to Aleynikov's acquittal may have been the result of something as simple as a congressional staff member inserting "pro forma 'interstate commerce'" text and choosing language that was more restrictive than was necessary.[244]

After the Second Circuit's ruling in *Aleynikov*, it is clear that the language of the EEA is too narrow to cover all of the activities that Congress presumably wanted to make illegal. One way of broadening Section 1832 would be to replace the "produced for or placed in interstate commerce" language with a requirement that the stolen material "substantially affect" interstate commerce. Amended this way, the statute would resemble other federal criminal laws whose definition includes a requirement that the crime "affect" interstate commerce, such as federal gun laws[245] or the Hobbs Act.[246] As the Second Circuit suggested, by making this change Congress could indicate its intention

240. *See* Lori J. Warner, *The Potential Impact of* United States v. Lopez *on Environmental Regulation*, 7 DUKE ENVTL. L. & POL'Y. F. 321 (1997) (arguing that certain provisions of the Clean Water Act and Endangered Species Act might face Commerce Clause challenges after *Lopez*); Michael Bablo, Note, Leslie Salt Co. v. United States: *Does the Recent Supreme Court Decision in* United States v. Lopez *Dictate the Abrogation of the "Migratory Bird Rule"?*, 14 TEMP. ENVTL. L. & TECH. J. 277 (1995) (arguing that the Migratory Bird Rule does not meet the Commerce Clause test set out in *Lopez*).

241. 529 U.S. 598 (2000).

242. 42 U.S.C. § 13981(b) (1994).

243. *Morrison*, 529 U.S. at 613.

244. POOLEY, *supra* note 18, § 13.03[3].

245. 18 U.S.C. § 922(g) (2006) (making it a crime to possess firearms, under certain conditions, that are "in or affecting commerce").

246. *See* 18 U.S.C. § 1951(a) (2006) ("Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion . . . .").

to "invoke the full extent of" its "regulatory power under the Commerce Clause."[247]

In its revised form, the EEA would reach far more activity than it currently does. In assessing whether criminal activity affects commerce, the courts have generally taken an expansive view. There are cases–such as *Lopez* and *Morrison*–in which a crime is regarded as so inherently localized that it does not meet the standard of affecting interstate commerce. In those rulings, however, the Court underscored what it saw as the limited connections between the underlying offenses–possessing a gun near a school or committing gender-motivated violence–and interstate commerce. The underlying offense in trade secret theft–taking valuable information from a business–is far more directly connected to interstate commerce, and courts would no doubt see it as such.

Alternatively, the EEA could be amended by inserting language requiring that the stolen material be "used in" interstate commerce. That is the approach the Senate took when it passed the Theft of Trade Secrets Clarification Act of 2012.[248] The Senate voted to strike the phrase "or included in a product that is produced for or placed in" and replace it with the words "a product or service used in or intended for use in" interstate commerce.[249] This change in language addresses the concerns raised in *Aleynikov*. The Second Circuit stated that products that are "placed in" commerce "have already been introduced into the stream of commerce and have reached the marketplace," and that products "produced for commerce" are ones that "are still being developed or readied for the marketplace."[250] The "used in" language eliminates the Second Circuit's emphasis on whether the stolen matter was in the marketplace or being developed for the marketplace. Instead, by making the issue whether the product or service was "used in or intended for use in" interstate commerce, the bill shifts the focus to the trade secret's function.

The language of the Senate bill would cover a far wider range of trade secret thefts. It would apply to the HFT source code that Aleynikov stole because, as the district court noted, "the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the Trading System was to engage in interstate and foreign commerce."[251] It would also cover technology companies' source codes and corporate R&D, because those too are intended for use in interstate commerce, whether or not they are headed for the marketplace themselves.

---

247. United States v. Aleynikov, 676 F.3d 71, 81 (2d Cir. 2012), *rev'g* 785 F. Supp. 2d 46 (S.D.N.Y. 2011).

248. Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (as passed by Senate, Nov. 27, 2012).

249. *Id.*

250. *Aleynikov*, 676 F.3d at 80.

251. United States v. Aleynikov, 737 F. Supp. 2d 173, 179 (S.D.N.Y. 2010).

B. Reining in the EEA

Congress should also consider the ways in which the EEA is overprotective. There was no dedicated federal trade secret law until 1996. When Congress decided to address the problem of trade secret theft directly by passing the EEA, it did so in an aggressive fashion. Rather than begin with a civil statute, which would have allowed it to wade gradually into a doctrinally fraught area of the law, Congress chose to enact a criminal law. Instead of closely tracking the state statutes and common law, or narrowing the scope of the conduct covered, Congress expanded trade secret law in a number of significant respects. And when it established the punishments for this broadly written statute, Congress went well beyond the level of sanctions included in state criminal trade secret theft statutes.

The aggressive stance of the EEA toward trade secret theft is problematic. As criminal law, the EEA has provisions that are vague and that over-punish. As business regulation, the EEA in important respects stifles innovation and has a negative impact on the labor market. And as information policy, the EEA is troubling because it is too protective of secrecy and too punitive toward releasing information that would benefit society.

1. The EEA as Criminal Law

The EEA over-criminalizes communicative activities, including within its coverage actions that, appropriately, have not traditionally been trade secret violations. The over-criminalization begins with the Act's definition of what constitutes a trade secret. Scholars and critics of the EEA have identified places in which the Act's definitions make it easier to find a defendant liable than under state law, as well as areas in which the definitions are too expansive.[252] The EEA's definition of a trade secret is so broad that it takes in a wide array of workaday commercial material, including customer lists and advertising plans. The EEA's vast definition of what constitutes a trade secret creates a danger of turning mundane acts of information sharing into major federal crimes. In some cases, these definitions create problems of notice, because workers and others may not have reason to know that federal criminal law has broken with traditional trade secret principles, and in other cases the definitions may simply be poor policy.

Another problematic aspect of the Act is the reference point it uses to define whether something is a trade secret. In the UTSA, a trade secret is defined as information that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, *other persons who can obtain economic*

252. *See supra* notes 115-133 and accompanying text.

value from its disclosure or use."[253] In the EEA, a trade secret is defined as information that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, *the public* . . . ."[254] The shift is significant, because those who can obtain economic value from business information are presumably more likely to know about the information than the general public. The expansion was not prompted by any legitimate business needs: for a company seeking to keep its secrets, the important question is whether its competitors have access to it. By loosening the definition, the EEA also creates the anomalous situation that prosecutors bringing serious criminal charges may have an easier case to make than plaintiffs bringing civil actions under state law.[255]

There are other ways in which the EEA is problematic as a criminal statute. Although the EEA has been held not to be unconstitutionally vague,[256] at least one federal district court has noted that it is "quite troubling" that under the Act "a 'trade secret' is based on intangible and evolving concepts and ideas," and phrases like "readily ascertainable" and "generally known" that are extremely ambiguous.[257] The EEA's forfeiture provisions also raise concerns because a trade secret may be only a small part of a larger product, but forfeiture would apply to the whole product. In some cases, "[c]onfiscating the invention or the profits derived from that invention could be grossly disproportionate to the technological contribution of the trade secret."[258]

In passing the EEA, Congress could have included a statutory minimum loss threshold. The NSPA applies only to cases in which stolen goods have a value of $5,000 or more,[259] and many other criminal and civil statutes have monetary thresholds. The original Senate version of Section 1832 applied only to the theft of "proprietary economic information having a value of not less than $100,000,"[260] but that language did not make it into the final bill. A statutory minimum could have helped to ensure that the law was only used for serious cases of trade secret theft. Given the vagueness of the statute, a statutory minimum might also have provided people some reassurance that they were not risking criminal prosecution when they used minor pieces of information culled from previous jobs.

---

253. UNIF. TRADE SECRETS ACT § 1(4)(i), 14 U.L.A. 438 (1990) (emphasis added).

254. 18 U.S.C. § 1839(3)(B) (2006) (emphasis added).

255. Moohr, *supra* note 71, at 878.

256. *See, e.g.*, United States v. Krumrei, 258 F.3d 535, 538-39 (6th Cir. 2001); POOLEY, *supra* note 18, § 13.03[2] n.12.1.

257. United States v. Hsu, 40 F. Supp. 2d 623, 630 (E.D. Pa. 1999).

258. Dreyfuss, *supra* note 52, at 30.

259. 18 U.S.C. 2314 (2006).

260. S. 1556, 104th Cong. § 2(a) (1996).

2. The EEA as Business Regulation

The EEA has been criticized for "effectively [swinging] the pendulum directly towards the interests of industry."[261] More accurately, it swung the pendulum toward the interests of trade secret holders, which is not necessarily the same thing. Industry's interest, and the national interest, when properly conceived, goes beyond locking down commercial secrets. In important ways, the EEA stifles innovation and entrepreneurship. It is also deficient as business regulation because of the deleterious effect it has on employees.

A strict and strictly enforced trade secrets regime can be an impediment to innovation. In a "leaky regime" of trade secrets, in which owners have less control over their information, other entrepreneurs are better able to assimilate that information into their own work and build on it. Patent and copyright laws are intentionally made "leaky"–with short durations in the case of the former, and fair use rules in the case of the latter–to allow this sort of building upon existing work. In many cases, it is "spillover," in which innovators from other fields interact with and expand on existing material, which produces the greatest advances.[262]

The EEA is in many respects far from a leaky regime. The statute's expansive and at times vague definitions of trade secrets put large amounts of material off-limits, and the heavy criminal penalties provide a strong incentive for would-be users of information to tread carefully. Unlike copyrights, where the information is made public and fair use is allowed, trade secrets are not part of a public informational ecosystem. Unlike patents, which expire after a fixed and relatively short period of time, trade secrets are off-limits for as long as the owner can manage to keep them secret.

One specific aspect of the EEA that has been criticized for impeding innovation is its ambiguous stance on reverse engineering–the process of creating similar or superior products by studying an existing product and determining how it was created. The EEA could be seen as prohibiting reverse engineering,[263] although the text and the legislative history are far from clear.[264]

If the courts ultimately hold that the EEA does bar reverse engineering, it would be a significant setback for innovation. Reverse engineering is generally considered an important tool for encouraging thought about how to improve upon existing technology and products. It is generally allowed in intellectual

261. Simpson, *supra* note 39, at 1134 ("Despite its lofty goals, the EEA is a bill that was clearly sponsored by, and passed to benefit, big business.").

262. Dreyfuss, *supra* note 52, at 34-35.

263. *See id.* at 15; Pooley et al., *supra* note 78, at 195.

264. *See* Uhrich, *supra* note 113, at 172-75. For the proposition that it was not Congress's intention to ban reverse engineering, *see* 142 CONG. REC. H10460-01 (daily ed. Sept. 17, 1996) (statement of Rep. Charles Schumer) (stating that the EEA was written so as to avoid including reverse engineering).

property regimes, and the trade secret laws of all states permit it.[265] At least one commentator, concerned that the EEA criminalizes reverse engineering, has proposed language for amending the Act.[266]

Another problem with the EEA as industrial policy is the effect it has on employees and, more specifically, employee mobility. There are many ways in which the law could reasonably put employees who take a new job in fear of being prosecuted for theft of trade secrets if they share knowledge that they acquired in previous jobs. The combination of vague statutory definitions and serious penalties could do this, as could specific provisions that broaden the scope of actions that could be illegal. One worrisome example is the Act's inclusion of taking confidential information through memorization. The EEA extends to "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored."[267]

Including theft by memory criminalizes an action that many people regard as a natural part of the movement from one job to another. States have taken different approaches to the question of whether memorization should be a basis for trade secret liability,[268] but most appear to limit criminal liability to cases in which there has been some kind of physical taking[269] and do not require employees to "wipe clean the slate of their memories."[270] Given the vagueness of the definition of trade secrets in many respects,[271] subjecting someone who has taken information from one job to another merely by memory to as much as ten years in prison seems excessive.

An early draft of the EEA expressly stated that the law could not be used to prosecute individuals who seek to capitalize on the knowledge, skills, or abilities they acquired on the job. That provision was dropped when the House and Senate versions of the bill were reconciled. The Managers' Statement for the House Bill said that Congress did not believe an express statement was necessary because of the requirements that a trade secret be something the owner took steps to protect, and that prosecutors point to a specific piece of stolen information.[272] Had the original language been retained, it would have given employees far stronger textual support for their right to share from their "toolkit" of knowledge and skills, and it would have reduced some of the fear among employees of being prosecuted by former employers.

---

265. Uhrich, *supra* note 113, at 167.

266. *Id.* at 186.

267. 18 U.S.C. § 1839(3) (2006).

268. *See* Rhonda DeVincent, Note, Ed Nowogroski Insurance, Inc. v. Rucker, *Is the Memory Rule Just a Thing of the Past?*, 7 SUFFOLK J. TRIAL & APP. ADVOC. 139 (2002).

269. *See* Lederman, *supra* note 79, at 966.

270. Moss, Adams & Co. v. Shilling, 179 Cal. App. 3d 124, 124 (1986). *But see* Morilife, Inc. v. Perry, 55 Cal. App. 4th 1514, 1525 (1997) (criticizing the *Moss* decision).

271. *See* Moohr, *supra* note 71, at 876-77.

272. 142 CONG. REC. S12,213 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. 3723, The Economic Espionage Bill).

The EEA can be seen as an example of the rise of "corporate intellectual property" and the decline of "artisanal independence."[273] The more the law regards information in a workplace as belonging to the corporation rather than the worker, the more risky it becomes for a worker to switch jobs. When it enacted the EEA, Congress stated that it did not intend to interfere with the ability of workers to bring a toolkit of general skills and information with them from job to job.[274] Despite that aspiration, it is not necessarily clear where the line between general skills and information and corporate intellectual property lies.[275] Making off with thousands of lines of computer code might well be a violation of the statute, but what about remembering some of the programming tricks used to write such code? Taking extensive lists of customers could easily be illegal theft of trade secrets. But what about making sales calls on customers that one has sold to in the past for a previous employer?

In the modern economy, it is increasingly rare for workers to spend a career with a single employer, and far more common for employees to make frequent job switches.[276] The EEA complicates this emerging employment picture because now workers who switch jobs must spend time trying to determine what information and techniques are properly part of their general knowledge base and, therefore, fair game for them to share with future employers. At the same time, they must carefully review what information they have that is a trade secret of their former employer–or might be something that the employer regards as a trade secret.

This process of sorting through one's personal store of business information, including that carried in one's own head, has become far more important since the enactment of the EEA because now the repercussions of being wrong about what information properly belongs to whom have become "quite a bit more severe."[277] Unfortunately for the worker, at the same time as the EEA has sharply increased the penalties for making the wrong assessment, it has adopted a number of definitions that are difficult even for judges to interpret.

Employees might in some cases reasonably decide that it makes more sense to stay put than to risk plying one's trade for a new employer and risk criminal prosecution. Simultaneously, the EEA changes the calculus for companies that are considering trying to hire away a competitor's workers. As

273. Catherine L. Fisk, *Working Knowledge: Trade Secrets, Restrictive Covenants in Employment, and the Rise of Corporate Intellectual Property, 1800-1920*, 52 HASTINGS L.J. 441, 445 (2001).

274. *See* United States v. Hsu, 155 F.3d 189, 196-97 (3d Cir. 1998).

275. POOLEY, *supra* note 18, § 13.03[6]; *cf.* United States v. Krumrei, 258 F.3d 535 (6th Cir. 2001) (rejecting vagueness challenge to EEA's requirement that trade secret owner take "reasonable measures" to protect it).

276. *See* Katherine V. W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 519 (2001).

277. POOLEY, *supra* note 18, § 13.03[6].

a result of the EEA, these workers may be less able than they once were to bring along valuable knowledge acquired at previous jobs. They may also be wary about sharing even information that they are within their legal rights to convey out of an excess of caution and a fear of the consequences of making the wrong assessment. Prospective employers, for their part, may be more reluctant to hire workers from the competition out of fear of being dragged into a criminal trade secrets prosecution.

The EEA could have a particularly significant impact on people who earn their livings as consultants. They are not merely making the occasional, carefully considered move from one employer to another. Their ordinary existence involves working for multiple companies at the same time and sharing with them knowledge acquired over the course of their career. In the best of circumstances, consultants are valued for their ability to "cross-pollinate" among clients, bringing best practices to a wide range of firms and increasing the efficiency of a whole industry.[278] This also has implications for individual workers. They are less likely to be able to command the full value of their labor when they have a diminished ability to exit to a rival firm. They are also less able to bargain for the best compensation package at the firm where they are currently employed if the law has contrived to define much of their skill base as belonging to the corporation, and if both the employer and employee know that the costs of exiting now include a risk of criminal prosecution.

Diminished labor mobility is costly not only for individual workers, but for the nation as a whole. The economy is at its most efficient when workers are able to take their labor where the market would value it most highly. In industries in which knowledge is paramount, labor mobility is of particular importance because it is the mechanism for inter-firm "knowledge spillovers."[279]

Professor Gilson has argued in a classic article that a major reason for California's Silicon Valley's greater success compared to Massachusetts's Route 128 is that Silicon Valley has legal rules that do more to encourage employee mobility.[280] His focus was post-employment covenants not to compete, but his analysis is in many ways parallel to trade secret law. An employment law regime that is structured to strongly favor the intellectual property rights of corporations makes it more difficult and costly for employees to move between firms. The relative arcs of Silicon Valley and Route 128 suggest the economic advantages of increased employee mobility. In this frame, the adoption of the EEA was to some degree a national move toward the

278. *Id.*

279. Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 578 (1999).

280. *See id.*

relatively inflexible legal regime of Route 128, rather than the more liberating one of Silicon Valley.

3. The EEA as Information Policy

Trade secret laws encourage people who have valuable information to keep it out of circulation and punish those who disclose it. There can be valid reasons for supporting a legal regime that allows people control over their proprietary business information,[281] but secrecy comes at a cost to public knowledge. If a trade secrets regime is too restrictive and its punishments too onerous, it can keep more information out of circulation than is socially beneficial.

The EEA is unduly restrictive in ways that are likely to exert a chilling effect on speech about business and industry. The Act's definition of trade secrets is sweeping, taking in not only scientific and technical information, but more run-of-the-mill subjects like customer lists, advertising plans, and personnel information. If the statute were more narrowly drawn, people would not have to worry when they spoke about matters like customers they served while working for a former employer, or the hiring and departure of executives. The broad scope of the EEA, however, means that workers discussing matters of this sort must be concerned about whether anything they say could become the basis for a criminal prosecution.

The Act's definition of misappropriation is also extremely broad. The EEA does not merely cover acts that appear obviously to be theft, like taking an employer's secret computer codes and handing them over to a competitor. It extends to information that is obtained in more benign ways, such as by observing a company from across the street, or speaking casually with current employees. It also covers information that an employee learned at a previous job and simply remembers. As a result, people engaging in ordinary talk about business, drawing on information they acquired by commonplace means, must worry about violating the Act. The EEA's chilling effect on information transfers is exacerbated by its heavy criminal penalties. Anyone who entertains the notion that her actions or conversations may be approaching the line of what is illegal is likely to be significantly deterred by the lengthy prison sentences that could result from a conviction.

The EEA's tough approach to trade secret theft, which Congress welcomed as a means of protecting industrial knowledge, comes at a price of diminished freedom of expression. The concerns about a trade secret law over-deterring speech weigh particularly heavily with certain kinds of information. Society may have less of an interest when the trade secret concerns something primarily of private economic value, for example an industrial "thing" such as a

281. *See supra* notes 17-28, 58-60, 68-69, 196-224 and accompanying text.

mold or a chemical process.[282] The concerns are greater, however, when the information being kept out of circulation would advance the public interest. That may be the case with certain kinds of business information that has value beyond its financial benefits, or even its contributions to innovation. An editor leaving one newspaper for another could be deterred from telling the new employer about the innovative journalistic practices he learned on old jobs if he was afraid of being charged with theft of trade secrets, and journalism could suffer. A health care provider might be wary of informing a new employer about certain kinds of best practices in patient care if she believed that a former employer might claim them as trade secrets.

There are some trade secrets in which the public interest in disclosure is particularly great. These include information that a product is unsafe or unreliable, a threat to the environment, or invasive of personal privacy.[283] There are many instances of tension between companies that want to keep commercial information secret and interests that want to be able to evaluate the environmental, health, and safety (EHS) risks of products.[284] When trade secret owners are allowed to shield this information, "[s]ociety as a whole sustains substantial losses and systematic distortions."[285] The EEA may tilt an employee's calculus on speaking out in some cases, because the fact that a product contains a potentially deadly mixture of chemicals, or that a car has an engine whose design puts it at risk of exploding, may be regarded as a trade secret, and disclosure could be regarded as a criminal act.

IV. Conclusion

The driving force in Congress for passing the EEA was a concern that foreign governments and foreign agents were stealing America's valuable trade secrets. The business community and elected officials got the strong criminal law they wanted in Section 1831, with broad definitions and heavy penalties. At the same time, supporters of a strong domestic criminal trade secret law also got what they wanted, in the form of Section 1832, although that section had a flaw–an unduly restrictive interstate commerce provision.

After the Second Circuit's ruling in *Aleynikov*, the weakness of Section 1832 is now clear–as is the way to fix it. Congress is currently in the process of

---

282. Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 780 (2007).

283. *See* Eugene Volokh, *The Trouble with "Public Discourse" as a Limitation on Free Speech Rights*, 97 VA. L. REV. 567, 579-80 (2011).

284. Mary Lydon, *Secrecy and Access in an Innovation Intensive Economy: Reordering Information Privileges in Environmental, Health, and Safety Law*, 78 U. COLO. L. REV. 465 (2007).

285. *Id.* at 467.

amending the EEA to address the interstate commerce concerns raised by the Second Circuit.[286]

Congress is right to try to plug the gap identified by the *Aleynikov* court, however, it should not stop with the interstate commerce provision. The EEA is a law that has a powerful impact not only on keeping business secrets confidential, but also on many other issues of considerable import, ranging from mobility of employees in the labor market to freedom to innovate, to the free flow of information across society. Congress does not appear to have given these matters the careful study and deliberation that they deserved before it enacted the statute. There are also issues with the definitions and other provisions of Section 1832, some of which stretch the scope of the federal criminal statute beyond the traditional limits of state civil and criminal trade secret laws.

It may be tempting to start drawing up language and suggesting amendments right away, such as revising the definition of trade secrets and clearing up ambiguities about matters like reverse engineering. But what Congress should do is not to start accepting proposed amendment language, but rather to put a deliberative process in place. Federal trade secret law has broad implications for many sectors of our society, and an important lesson of the *Aleynikov* ruling is that hastily drawn-up legislation can fall short of what is needed.

Congress should hold hearings on proposed amendments to the EEA presided over by committees dedicated to intellectual property law, not criminal law enforcement. It should hear from a wide array of experts in business, the academy, and law enforcement, as well as interested members of the general public. It should then enact a revised EEA that does not simply plug a hole, but rather thoroughly reworks it to be both more inclusive and less inclusive–and in the right ways.

286. *See* Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (as passed by Senate, Nov. 27, 2012).